PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04J 3/14, F06F 11/00

A1

(11) International Publication Number: WO 00/07312

(43) International Publication Date: 10 February 2000 (10.02.00)

(21) International Application Number: PCT/US99/17408

(22) International Filing Date: 30 July 1999 (30.07.99)

(30) Priority Data:
09/127,241 31 July 1998 (31.07.98) US

(71) Applicant: GTE GOVERNMENT SYSTEMS CORPORATION [US/US]; Intellectual Property Department, 1209 Orange Street, Wilmington, DE 19801 (US).

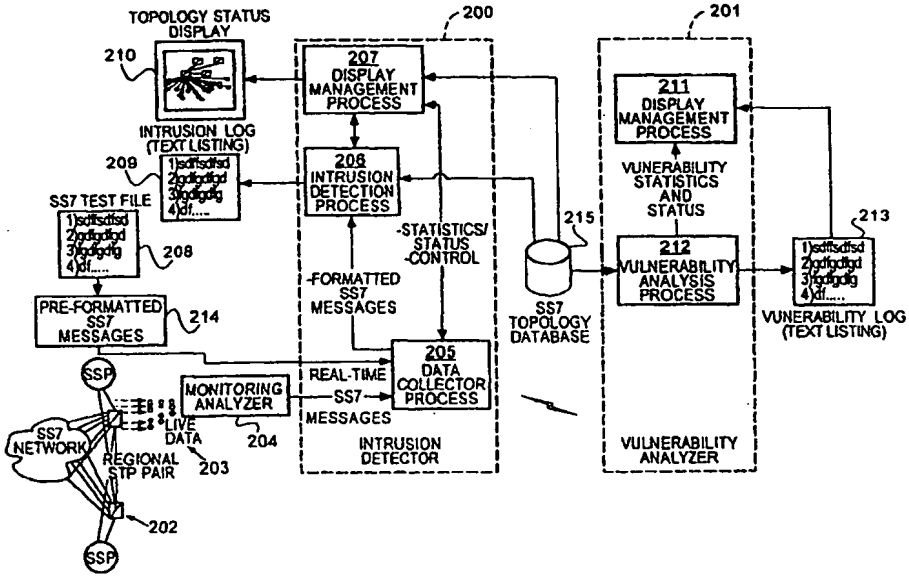
(72) Inventors: GORMAN, David, B.; 11612 Happy Choice Lane, Gaithersburg, MD 20878 (US). CATHERINE, Gregory, J.; 11432 Herefordshire Way, Germantown, MD 20876 (US). PERAGINE, Richard; 3 Silktree Court, Catonsville, MD 21228 (US). CONRAD, Beverly; 7 Brooking Court #302, Timonium, MD 21093 (US). GEARHART, G., Duane; 3-J Cameron Court, Baltimore, MD 21236 (US). MOY, David; 7033 Cradlerock Farm Court, Columbia, MD 21045 (US).

(74) Agents: ANDERSON, Floyd, E. et al.; GTE Service Corporation, 600 Hidden Ridge Road, MC HQE03G13, Irving, TX 75038 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.
With amended claims.

(54) Title: SYSTEM FOR INTRUSION DETECTION AND VULNERABILITY ANALYSIS IN A TELECOMMUNICATIONS SIGNALING NETWORK



(57) Abstract

Detecting (206) attempted intrusions in a telecommunications signaling network (202) and assessing (212) the vulnerability of the network to the attempted intrusions. Intrusion rules are applied to received messages in the network in real-time, using a known protocol for the network, in order to detect anomalies tending to indicate an attempted intrusion. In order to assess the vulnerability of the network, the vulnerability rules are applied to rankings of particular parameters relating to elements in the network. The rankings provide an indication of susceptibility of a network element to an attempted intrusion relative to other network elements.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

SYSTEM FOR INTRUSION DETECTION AND VULNERABILITY ANALYSIS IN A TELECOMMUNICATIONS SIGNALING NETWORK

Technical Field

The present invention relates to a system and method for detecting intrusion into, and for assessing the vulnerability of, a telecommunications signaling network.

Background Art

Telecommunications signaling networks are susceptible to intrusion, meaning that a person may use software or physical means to cause disruption or denial of service within the network. For example, a person may use software operating on a computer in an attempt to seize control of a particular node or link in the network and consequently cause a disruption or denial of service. As another example, a person may attempt to take physical control of an entity in the network, such as a link, resulting in a disruption or denial of service.

These intrusions create an undesirable situation for communications service providers and for customers using the network. In particular, the disruptions or denials of service may inconvenience customers and potentially cause a loss in revenue for the communications service provider. When a disruption occurs, a service provider may attempt to locate the disruption and determine a cause of the intrusion. However, in that case the service provider only obtains an indication of the intrusion after it has already caused a disruption and thus cannot anticipate such an intrusion before it occurs. In addition, the server provider may not necessarily know in advance which portions of the network are most susceptible to an intrusion and thus not know how to best monitor the network for potential intrusions.

Accordingly, a need exists for detection of intrusion in a telecommunications signaling network, potentially in real-time, and for analysis of the vulnerability of the telecommunications signaling network to an intrusion.

Brief Description of the Drawings

FIG. 1 is a diagram of an exemplary telecommunications signaling network and associated machine for monitoring the network;

FIG. 2 is a diagram of software modules operating on the machine shown in FIG. 1 for implementing an embodiment consistent with the present invention;

FIG. 3 is a flow chart of an exemplary process for monitoring a telecommunications signaling network for intrusion detection;

FIG. 4 is a flow chart of an exemplary process for determining vulnerability of a telecommunications signaling network to potential intrusion;

FIG. 5 is an exemplary user interface for entering set-up information for an intrusion detection process;

FIG. 6 is an exemplary user interface for displaying status information related to an intrusion detection process; and

FIG. 7 is an exemplary user interface for displaying information related to a vulnerability analysis of a telecommunications signaling network.

Disclosure of Invention

Apparatus and methods consistent with the present invention provide indications of attempted intrusions in a telecommunications signaling network and the vulnerability of particular elements in the network to attempted intrusions.

An apparatus consistent with the present invention receives messages related to communications in a telecommunications signaling network. The apparatus applies intrusion rules to the messages in order to order to detect anomalies in the messages, and it reports an indication of the detected anomalies.

Another apparatus consistent with the present invention receives rankings for particular parameters related to elements of a telecommunications signaling network. The apparatus applies vulnerability rules to the rankings in order to determine a likelihood of an attempted intrusion into the corresponding elements of

the telecommunications signaling network, and it reports an indication of the likelihood of the attempted intrusions.

A method consistent with the present invention includes receiving messages related to communications in a telecommunications signaling network. Intrusion rules are applied to the messages in order to order to detect anomalies in the messages, and an indication of the detected anomalies is reported.

Another method consistent with the present invention includes receiving rankings for particular parameters related to elements of a telecommunications signaling network. Vulnerability rules are applied to the rankings in order to determine a likelihood of an attempted intrusion into the corresponding elements of the telecommunications signaling network, and an indication of the likelihood of the attempted intrusions is reported.

Best Mode for Carrying Out the Invention

Apparatus and method consistent with the present invention provide indications of attempted intrusions in a telecommunications signaling network and the vulnerability of particular elements in the network to attempted intrusions. Although both intrusion detection and vulnerability analysis are described, each is typically a separate entity, and the operation of one is not necessarily dependent on the other.

Attempted intrusions refers to attempts to disrupt or deny service in the network or to otherwise tamper with the network. Intrusion rules are applied to received messages in the network, typically in real-time and using a known protocol for the network, in order to detect anomalies tending to indicate an attempted intrusion. Messages refers to any particular data element transmitted in the network. For example, standard telecommunications signaling networks use messages in order to provide particular telephone-related services to customers. Intrusion rules refers to any criteria or methodology for detecting the anomalies. Indications of the

attempted intrusions may be presented, for example, in a user interface that includes a topological representation of a monitored portion of the network.

In order to assess the vulnerability of the network, vulnerability rules are applied to rankings of particular parameters relating to elements in the network. Vulnerability rules refers to any criteria or methodology for processing the rankings to provide indications of likelihood of attempted intrusions with respect to particular elements in the network. Rankings refers to any information providing an indication of susceptibility of a particular network element to an attempted intrusion relative to one or more other network elements. A user interface may be presented in order to receive the rankings and to display indications of the vulnerability of elements in the network.

FIG. 1 depicts a data processing system 100 suitable for practicing methods and systems consistent with the present invention. Data processing system 100 includes a machine 101 for intrusion detection and vulnerability analysis, connected to a network 107 such as a private or public telecommunications signaling network. Machine 101 includes a memory 102, a secondary storage device 104, a processor 105 such as a central processing unit, an input device 106, and a display device 103. Memory 102 and secondary storage 104 may store applications and data for execution and use by processor 105. Input device 106 may be used to enter information and commands into machine 101, and display device 103 provides a visual of information in machine 101.

Although machine 101 is depicted with various components, one skilled in the art will appreciate that this computer can contain additional or different components.

Additionally, although machine 101 is shown connected to network 107, machine 101 may be connected to other networks, including other wide area networks or local area networks. Furthermore, although aspects of the present invention are described as being stored in memory, one skilled in the art will

appreciate that these aspects can also be stored on or read from other types of computer program products or computer-readable media, such as secondary storage devices, including hard disks, floppy disks, or CD-ROM; a carrier wave from the Internet; or other forms of RAM or ROM. In addition, the computer-readable media may include instructions for controlling a computer system, such as machine 101, to perform a particular method.

FIG. 2 is a diagram of software modules operating on the machine shown in FIG. 1 for implementing an embodiment consistent with the present invention. These modules include modules 200 for intrusion detection and modules 201 for vulnerability analysis of a network 202. Network 202 is a standard Signaling System 7 (SS7) protocol network and illustrates an example of network 107. Other examples of network 107 include an integrated Services Digital Network (ISDN) and an X.25 network. A monitoring analyzer module 204 receives real-time data 203 from network 202. Real-time data 203 may include messages transmitted in an SS7 protocol network or other type of network. Monitoring analyzer 204 packages the data for analysis and forwards it in real-time to a data collector process module 205. Data collector process module 205 parses the received data to remove information from the messages not necessary for intrusion analysis, and it reformats the parsed messages to a consistent format to facilitate intrusion analysis. Data collector process module 205 alternatively may receive preformatted SS7 protocol messages 214 from a test file 208 for use in testing or verifying the intrusion detection capabilities of the system.

An intrusion detection process module 206 receives the reformatted messages and performs processing of the messages to detect intrusion. In particular, it applies intrusion detection rules to the messages in order to detect anomalies in the messages or other events tending to indicate an attempt at intrusion into the network or to otherwise tamper with the network. These rules may be stored in memory or in a

database such as memory 102 or secondary storage 104, or they may be implemented in hard-wired logic.

Examples of these rules are provided in the Appendices. After or during performance of the intrusion detection processing, intrusion detection process 206 outputs the results to an intrusion log 209 that maintains a time-stamped history of the processing in the form of a textual listing, and it outputs the results to a display management process module 207. The textual listing may be printed in hard copy form using a printer connected to machine 101 or may be displayed on display device 103.

Display management process module 207 formats the processed data for display within a topology status display 210, which may be displayed by display device 103. Topology status display 210 provides a visual indication of the status of the monitored network and indications of intrusions into the network, and an example of a user interface for the topology status display is described below.

A topology database 215 stores information representing a topology or interconnectivity of network 202. Intrusion detection process module 206 and display management process module 207 may access database 215 in order to retrieve the topology information and use it in the processing performed by those modules. In addition, topology database 215 may store the rules used by intrusion detection process module 206. Topology database 215 may correspond to secondary storage 104, and it may be implemented, for example, with a Sybase database.

Vulnerability analyzer modules 201 include a vulnerability analysis process module 212 and a display management process module 211. Vulnerability analysis process module 212 receives the network topology information from topology database 215, and it applies vulnerability rules to the topology information in order to determine the vulnerability of elements in network 202 to intrusion attempts. Examples of these rules are provided in the Appendices. Vulnerability analysis

process module 212 outputs the results of its analysis to a vulnerability log 213, which maintains a time-stamped textual history of the processing in the form of a textual listing, and it also outputs the results to a display management process module 211. The textual listing may be printed in hard copy form using a printer connected to machine 101 or may be displayed on display device 103.

Display management process module 211 operates in a similar manner as module 207. In particular, it receives output results from module 212 and formats the received data for presentation in a user interface by display device 103. An example of a user interface for presenting the vulnerability process data is described below.

FIG. 3 is a flow chart of an exemplary process 300 for monitoring a telecommunications signaling network for intrusion detection. Process 300 may be implemented on machine 100 operating under control of intrusion detector modules 200 and module 204. In process 300, the system receives communication messages from the network such as SS7 messages provided by monitoring analyzer module 204 from network 202 (step 301). The system parses and formats the messages using data collector process module 205 (step 302). Intrusion rules are applied by intrusion detection process module 206 to the formatted messages to detect anomalies or other events in the network tending to indicate an attempted intrusion (step 303). The results are reported and potentially displayed by display device 103, using intrusion log 209 or topology status display 210, to provide a visual indication of attempted intrusions into network 202 an potentially the status of the network (step 304).

FIG. 4 is a flow chart of an exemplary process 400 for determining vulnerability of a telecommunications signaling network to potential intrusions. Process 400 may be implemented on machine 100 operating under control of vulnerability analyzer modules 201. Process 400 operates by using static rankings

processed as input weightings according to particular rules to generate further rankings. The process may be performed iteratively such that the output from one particular processing rule may be input as a ranking to another rule. The boxes in process 400 represent static rankings for particular parameters related to the network, and the circles represent vulnerability rules for processing the rankings. Examples of these vulnerability rules are provided in the Appendices.

Examples of parameters providing rankings as particular weightings for processing by vulnerability rules include the following: a percent utilization 401, a number of links 402, a percent traffic external 403, a monitoring 404, a screening 405, a media type 406, a transmission provider 407, a services 411, a user service rank 413, a connectivity by service 414, a node occupancy by service 416, and a user SSP ranking 418. These parameters are explained in the Appendices, and different or additional parameters may be used to perform a vulnerability analysis of a telecommunications signaling network.

Each parameter produces a static rank, in this example a particular number, to be processed by vulnerability rules. A functional capacity rank rule 408 receives inputs from parameters 401-404 and produces a result according to the function of rule 408. A security rank rule 409 receives inputs from parameters 404 and 405 and produces a result according to the function of the 409. A physical access rank rule 410 receives inputs from parameters 406 and 407 and produces a result according to the function of rule 410. A functional services rank rule 412 receives as input parameters 411 and 404, as well as the output from rule 409, and produces a result according to the function of rule 412. The process continues iteratively as an inherent link ranks rule 420 receives the outputs from rules 408, 409, 410, and 412, and produces a result according to the function of rule 420. Rule 420 provides one input to a most critical links rule 422.

The following provides the other input to most critical links rule 422. An SCP criticality rule 415 receives as inputs parameters 413, 414, and 416, and it produces a result according to the function of rule 415. An STP criticality rule 417 receives as inputs parameters 414 and 416, and the output of rule 415, and it produces a result according to the function of rule 417. An SSP criticality rule 419 receives as inputs parameters 414, 416, and 418, and it produces a result according to the function of rule 419. As the process proceeds iteratively, a most critical nodes rule 421 receives the outputs from rules 417 and 419, and it provides the other input to most critical links rule 422. Therefore, as a result of this iterative process, the result of rule 422 provides an indication of the most vulnerable link in the network, and the result of rule 421 provides an indication of the most vulnerable node in the network, the phrase "most vulnerable" meaning that it is the element most likely to be susceptible to an attempted intrusion.

FIG. 5 is an exemplary user interface 500 for use in entering set-up information for an intrusion detection process such as process 300. User interface 500 may be displayed on display device 103. User interface 500 includes a first section 501 used to receive threshold values for detection of intrusion, a second section 502 used to identify a point in the network from which the intrusion detection process receives data, and a third section 503 used to save and retrieve set-up information so that a user need not repeatedly enter the same set-up information. A user may enter relevant information into sections 501 and 502 using input device 106, and section 502 identifies where data 203 originates in network 202 and thus provides a reference point for performing an intrusion detection process. The location where the data originates may typically be changed so that a user may monitor the network from varying locations, and the location may be selected by using, for example, results of a vulnerability analysis.

FIG. 6 is an exemplary user interface 600 for displaying status information related to intrusion detection such as information produced by process 300. User interface 600 may be displayed on display device 103. User interface 600 includes a main section 601 for displaying a topological representation of a portion of the network and including information indicative of various conditions in the network. These conditions may provide an indication of attempted intrusions in the network. A displayed node 602 corresponds to the node identified in section 502 of user interface 500, and node 602 represents the node from which the system receives data. Other displayed nodes 603 and 604 represent nodes located one link away from node 602 in the monitored network. Each of the displayed nodes includes associated point codes and link information, displayed adjacent the corresponding node. Section 601 also displays lines between the nodes, and the lines represent the corresponding links.

When a user selects a particular displayed node the system displays a section 605 for presenting node information relating to the selected node. The node information may include a ranking determined by a vulnerability analysis. When a user selects a displayed link, the system displays a section 606 for presenting static information relating to the selected link, including link attributes, an anomaly history, and a linkset selection label. The anomaly history may correspond to history log 209. The user may select a particular node or link by, for example, using a cursor-control device to "click on" the particular node or link.

The system may optionally present the links in different colors to provide indications of varying conditions. For example, it may present the links using the following colors: green for a normal condition; yellow for a minor condition; orange for a major condition; red for a critical condition; and gray to indicate that the link is not monitored. The various conditions may be determined by the detected anomalies

from module 206 and particular predefined thresholds, which are further explained in the Appendices.

FIG. 7 is an exemplary user interface 700 for displaying information related to a vulnerability analysis such as process 400. User interface 700 may be displayed on display device 103. User interface 700 includes various sections in which a user may enter rankings for use by the rules in process 400. For example, it includes a section 701 to receive values for a services ranking and a section 702 to receives values for an SSP ranking. A user may select an appropriate tab 703 on a menu bar to view the corresponding section 701 and 702. User interface 700 may include additional tabs 703 and sections for receiving information concerning other rankings.

The accompanying Appendices, which are incorporated in and constitute a part of this specification, include the following: Appendix A includes a system overview for an exemplary intrusion detection process and vulnerability analysis; Appendix B includes a software user's manual for an exemplary intrusion detection process and vulnerability analysis; Appendix C includes a software design document for an exemplary intrusion detection process and vulnerability analysis; Appendix D includes a description of exemplary vulnerability analysis attributes and algorithm, including vulnerability rules; and Appendix E includes a description of exemplary intrusion detection algorithms including intrusion rules.

APPENDIX A
SYSTEM OVERVIEW

TABLE OF CONTENTS

APPENDIX A
SYSTEM OVERVIEW

LIST OF FIGURES

APPENDIX A
SYSTEM OVERVIEW

1. Scope

1.1 System Overview

Signaling System 7 (SS7) is the Control Service Layer of the Public Switched Telephone Network (PSTN); therefore, an attack on the SS7 network can cause PSTN service disruption /denial without undertaking a physical attack. An attack on the SS7 network can actually be accomplished through the manipulation and exploitation of the SS7 message protocol itself by means of message insertion onto the network signaling links. The SS7 network is inherently vulnerable to such attacks for two (of several) reasons: the SS7 protocol does not include Security and SS7 was built for robustness and thus, is very forgiving to anomalous states.

The System includes two tools: an SS7 Intrusion Detection Tool and a Vulnerability Analysis Tool.

The operational concept is that the intrusions would be well organized with the intent of service disruption/ service denial through insertion of SS7 messages into the SS7 message traffic stream. Due to the 'equal access' provision of the 1996 Telecommunications Reform Act, concern within the PSTN industry has increased over the fear of new and unknown carriers entering the market. These unknown entities pose a new threat to the SS7 network since they can demand full interconnection capabilities into the existing SS7 network while providing only limited visibility into their operations. Hence a modestly funded operator could gain full access the SS7 network for illicit purposes.

1.1.1 Vulnerability Analysis Tool

The purpose of the System SS7 Network Vulnerability Analysis Tool is to allow the user to determine which network elements in the SS7 Network are most vulnerable to an SS7 Message Insertion attack designed for Service Disruption/ Denial. As the analysis relates to Intrusion Detection, the results are used to indicate where Intrusion Detection resources should be applied in the Network based on the evaluated preferences supplied by the operator.

The Vulnerability Analysis Tool uses an SS7 Network Topology database which contains a set of attributes describing all of the SS7 Network Elements (links and nodes). These Network Element attributes are evaluated against a set of attribute weighting factors and against formulas relating combinations of attributes. The user has the ability to modify attribute weightings to tailor the analysis for specific preferences.

1.1.2 Intrusion Detection Tool

The real-time SS7 Intrusion Detection Tool provides SS7 link monitoring and analysis of SS7 message traffic for anomalous events which indicate possible intrusion into the message stream. The Intrusion Detection algorithms apply rules based logic and event thresholding against the message traffic stream. The logic evaluates message sequence and timing irregularities, inconsistent parameter values, and exceeded thresholds of message type occurrences.

The User Interface includes of a Network Topology display of the monitored network nodes and corresponding signaling linksets. The linkset status is indicated to the user by coloring the link icons corresponding to the severity of the detected anomaly. The detected anomaly text is displayed to the user in an Alarm Status window.

APPENDIX A
SYSTEM OVERVIEW

1.1.3 Network Topology Database

One of the goals of the system program has been to base the tools on real SS7 network data and operations. In order to accomplish this, the system has incorporated GTE Telephone Operations (TELOPS) network topology data and operational statistics into the system database.

2. References

The following documents provide background information and are incorporated herein by reference:

	DOCUMENT No.	TITLE
[1]	ANSI T1.111-1992	Signaling System Number 7, Message Transfer Part (MTP), American National Standards Institute Inc., 1992
[2]	ANSI T1.113-1995	Signaling System Number 7, ISDN User Part (ISUP), American National Standards Institute Inc., 1995

3. Intrusion Detection Tool

3.1 Concept of Operation

The Intrusion Detector examines the SS7 network messages and identifies anomalous conditions that may indicate message insertions into the SS7 stream. Such conditions are detected by identifying inconsistencies in the message parameters, message sequences, and by thresholding message occurrences.

The Intrusion Detector operates in the manner of a network management system. Therefore, the graphical user interface (GUI) provides a topological view of the network being monitored. Detected anomalies are indicated to the user by coloring the links on the topological map.

3.1.1 Concept of Execution

The Intrusion Detector analyzes each new message received and examines several aspects. Along with the information contained within the newly received SS7 message itself, the detector uses the information from previously captured SS7 messages, as well as network topology information.

- Message parameters against topology information are the point codes consistent with how the nodes are linked.
- Number of occurrences of the specific message type against the user defined threshold
- Message sequence inconsistencies either due to the intrusion message itself or as a result of the nework reacting to the intrusion message.

The following conditions are tested at different levels of the protocol:

a) ISDN User Part (ISUP) messages (See reference [6])
   - i) Improper RELEASE
   - ii) Improper BLOCKING and/or CIRCUIT GROUP BLOCKING
   - iii) Improper RESET and/or CIRCUIT GROUP RESET
   - iv) Improper FACILITY DEACTIVATED
   - v) Improper UNIDENTIFIED CIRCUIT IDENTIFICATION CODE

b) Message Transfer Part (MTP) messages
   - i) Improper CHANGEOVER (including Emergency Changeover)
   - ii) All improper MANAGEMENT INHIBITING

APPENDIX A
SYSTEM OVERVIEW

iii) Improper SIGNALING ROUTE MANAGEMENT (Transfer-Prohibited and Transfer-Restricted only)

Whether there was an anomaly detected or not, the current SS7 message is finally stored, to be used in the next anomaly test.

3.1.2 Interfaces

The context diagram, shown in Figure 3-1, identifies the multiple subsystem processes. The following subsections address these interfaces, with the exception of the Data Collector input

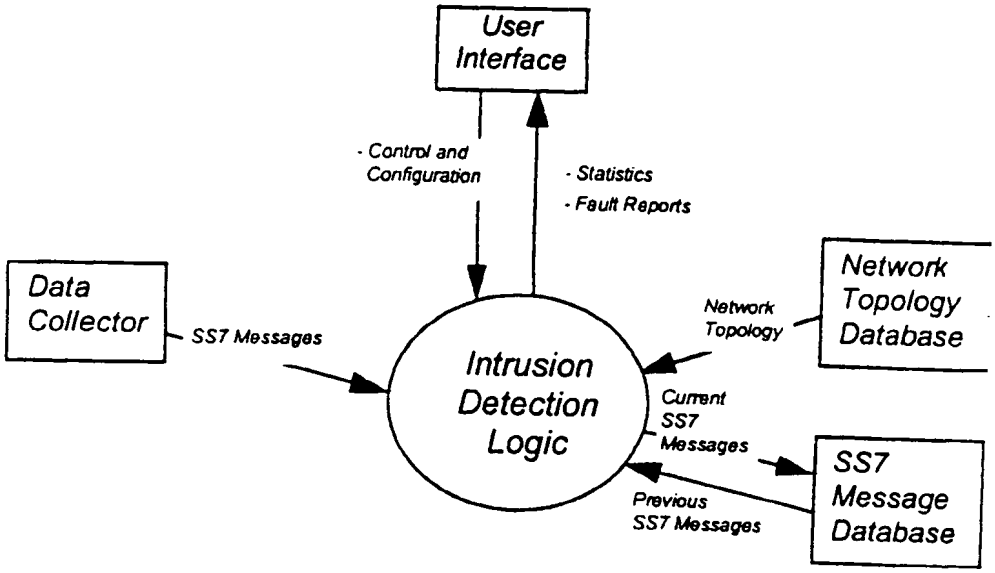


Figure 3-1 - Intrusion Detector Context Diagram

3.1.2.1 Graphical User Interface (GUI)

The GUI is the mechanism used to allow the system operator to configure the system, start and stop operations and provides the message analysis results on a topological status display. The design reflects a network management type display to the user. As with such systems, a network topology display depicts the network elements (in this case SS7 nodes and links).

Upon initialization of this process, the GUI retrieves configuration and network topology information from the corresponding databases to construct a view of the local SS7 network infrastructure (nodes, signal links, etc.), relative to the link being monitored.

This view is used to communicate to the operator the current state of each link of that local network. All direct links, to the link being monitored, are represented by a dashed line. The link being monitored is represented by a solid line to differentiate itself.

Network status is displayed by coloring the links. Node information and link status windows provide greater detail of the network.

3.1.2.1.1 Control and configuration

APPENDIX A
SYSTEM OVERVIEW

In response to a control message from the GUI subsystem, the Intrusion Detector accepts the following information from the GUI message queue for configuration and control:

a) START operation
b) STOP operation
c) PAUSE operation
d) Send Status/Statistic data
e) Threshold and parameter values for algorithms

3.1.2.1.2 Status and Statistics

When any of the predefined anomaly rules or a combination of these rules are satisfied (indicating an anomaly), a message is sent to the GUI input queue for display. The message will indicate the following information about the anomaly:

a) the SS7 message (protocol analyzer output format)
b) a time stamp generated by the Data Collector
c) the rule(s) fired that caused the anomaly report
d) the link affected and the color code indicating the anomaly ranking (GREEN, YELLOW, ORANGE or RED) as displayed to the operator

3.1.3 Data Collector

The Data Collector accepts SS7 message data from both a protocol analyzer and a test file source. It is a real-time operation, which is comprised of thee primary functions: the Message Parser, the input stream multiplexer and the output message queue.

The complexity of this subsystem is minimal, however, partitioning of the collection functionality enables the possibility of porting it to another processor, if the performance is required. Also, it isolates the impact to the other subsystems if there are hardware changes to the front-end collection method (e.g., change of protocol analyzer).

3.1.3.1 Concept of Execution

The Data Collector can manage inputs from a live message stream from a protocol analyzer source, or from a test file, or both. When accepting inputs from a protocol analyzer, the Message Parser is invoked to reformat the SS7 data into a condensed format needed by the Intrusion Detector process. When live data is combined with test file data, the test file data must be multiplexed into the live data stream. This combined mode is useful since it allows injection of test SS7 intrusion messages against a background of live nominal SS7 messages. In this manner, the Intrusion Detector can be tested against real message traffic (and message traffic volume) and still be able to test specific intrusion scenarios without the need to inject anomalies onto the actual network.

APPENDIX A
SYSTEM OVERVIEW

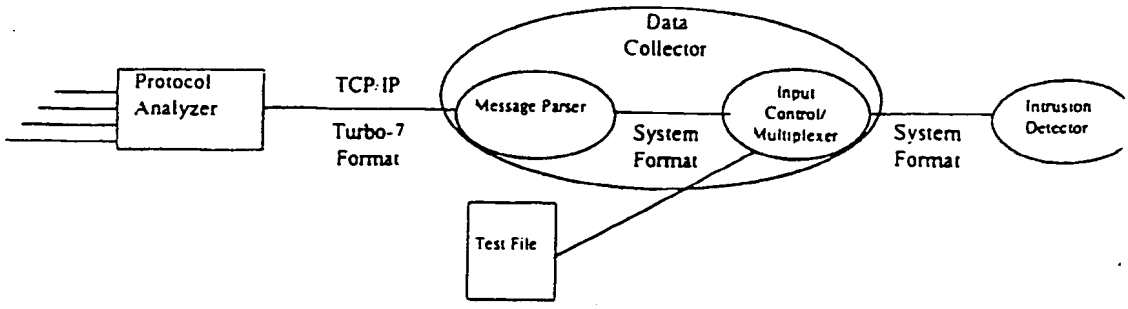


Figure 2 Data Collector Path

3.1.3.1.1 Protocol Analyzer

The protocol analyzer uses an INET Turbo-7 with an MSU Forwarding option. The MSU Forwarding feature provides TCP/IP forwarding capability of the collected SS7 Message Signal Units (MSU's).

The Turbo-7 protocol analyzer outputs the SS7 as received in time sequence from all of the monitored SS7 links. Each message has a header including of the port and timestamp followed by the raw SS7 message. The Turbo-7 outmessage format is shown in the Software User's Manual.

3.1.3.1.2 Message Parser

The Message Parser operates as a go-between from the protocol analyzer and the Intrusion Detector process. The input from the protocol analyzer is received over a TCP/IP socket interface. Each message is analyzed and reformatted by message type, retaining only those parameters required by the Intrusion Detector process. If additional message types and/or message parameters are desired or if different message collection hardware is used, the Message Parser can be modified without impact to follow on processes.

3.1.3.2 Test Files

The test files allow the Intrusion detector to run in a testing / simulation configuration when it is not desired or when it is impractical to have a live network connection. The test file is simply a concatenated set of SS7 messages in the data format output by the Message Parser. The messages can represent data from any protocol analyzer port with any values desired in the data fields. Therefore, test files can be set up to emulate normal SS7 network traffic on a variety of signaling links with embedded anomalies.

Although the test files use data formats output by the Message Parser, there is one distinction: the timestamp field. The test file timestamp field represents a time delay vice an absolute time. This convention was established in order to accommodate both a real time aspect to the test data timing and to facilitate test file message injection into the live data stream. Test file formats are described in the Input MSU Test File section of the Software User's Manual.

APPENDIX A
SYSTEM OVERVIEW

3.1.4 Network Topology Database

The Network Topology Database provides the intrusion detection algorithms with the required relevant infrastructure data of the SS7 network. The network topology information and its format, is described in the Software User's Manual.

The topology data is used by the Intrusion Detector to perform several types of legitimacy checks of the message point codes. Basically, checks are made to ensure that the messages are originating from legitimate locations and are arriving over the proper routes. These checks are based on message type.

4. Vulnerability Analyzer

The primary responsibility of the Vulnerability Analyzer is to evaluate an SS7 infrastructure data and determine the locations most vulnerable to SS7 network intrusion. The goal was to produce a tool that evaluated the network vulnerability in the same manner as a network analyst evaluates the network. To demonstrate the ability to evaluate different operational priorities, the user is able to designate certain evaluation parameters.

4.1 Concept of Execution

In response to a START message sent to its message queue from the User Interface, the analyzer retrieves network topology information from the database. These Network Element attributes are evaluated against a set of attribute weighting factors and against formulas relating combinations of attributes. The attributes are stored in the topology database whereas the rankings are stored in a configuration file. (Refer to the Software Users Manual for descriptions.)

The user has the ability to modify attribute rankings to tailor the analysis for specific evaluation preferences such as:

- select whether to evaluate Advanced Intelligent Network (AIN) services or Plain Old Telephone Service (POTS)
- when AIN is selected, rank the AIN services relative to each other to indicate the service(s) that have greater importance to the evaluation
- select specific SSP locations and rank those locations higher than nominal to indicate customer(s) locations that may have greater importance to the evaluation (such as government or business groups)

The evaluation formulas have been implemented within the software. Below is an outline of the analysis logic that is performed. Every attribute of every node and link within the network is evaluated. A base score of each node and link is established and is subsequently modified at each stage of the evaluation. The influence to the vulnerability score of each attribute is determined by the value of the attribute and on the importance ranking of that attribute. The rankings act as a weighting applied to the attribute value within the formula and control how much of a modifier of the attribute to the overall vulnerability score. As each node and link is evaluated, combinations of attributes are also evaluated and ranked.

The criteria for determining most critical node is that which attains a score of 10 or above. If more than one node is identified as exceeding a score of 10 than each node is listed with the corresponding list of vulnerable links to that node. (This is due to determining the number of hops to the critical node from each link).

APPENDIX A
SYSTEM OVERVIEW

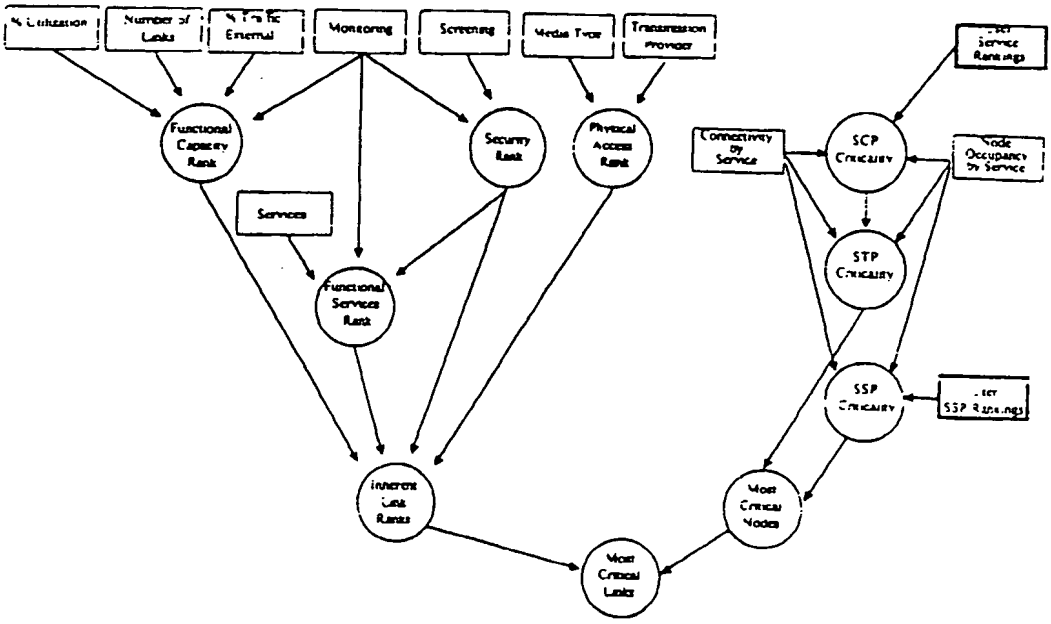


Figure 3: Vulnerability Analysis Logic Flow

4.1.1 Node Evaluation

The nodes are primarily evaluated to determine their criticality to the overall network operations and thus desirability to attack.

In the case of POTS evaluation, each STP pair is evaluated based on the number of SSPs directly connected to the STP and the volume of the SS7 traffic routed through the STPs.

For AIN cases, the evaluation is more complicated since the network becomes hierarchical with parent-child relationships formed among the STPs organized by the routing to each specific service. Therefore, node criticality becomes a function of not only the number and traffic from directly connected SSPs but also the number of SSPs indirectly connected that also gain access to the AIN service through the STP.

Following the criticality evaluation, certain inherent vulnerability attributes are also evaluated, such as:

- whether a node is owned or operated by a non-GTE entity is evaluated has the vulnerability increased by some measure. The ranking is applied by company.
- whether the node is occupied by personnel and by how many (physical control)
- how many backup nodes are available for auto rerouting.

4.1.2 Link Evaluation

The overall evaluation of the links is in effort to assess the inherent vulnerability to inserting messages onto the links to gain access to the critical nodes. However, the links are also evaluated on the criticality attributes related to traffic load and by service. Therefore, the user service rankings also influence the link vulnerability. This functional capacity ranking is used throughout the evaluation to modify the other

APPENDIX A
SYSTEM OVERVIEW

inherent vulnerability attribute scores. At the end of the inherent link vulnerability analysis, the links are modified one last time by the number of hops the link is from the critical node The concept being that the greater number of hops from the target the less likely the inserted message will reach the intended target.

The majority of the link attributes relate to inherent vulnerabilities of the links to SS7 message insertions aimed at affecting the critical nodes. Some examples are listed below:

- physical media addresses the concept of a physical tap into a link and the relative accessibility of : coax vice fiber.
- whether the transmission facilities are operated by a non-GTE entity is evaluated has the vulnerability increased by some measure. The ranking is applied by company, since some are more trusted than others.
- amount message traffic originating external to the GTE network and therefore coming from potentially unknown sources.
- whether STP screening is invoked and the robustness of the screening logic

4.2 Interfaces

The context diagram, shown in Figure 4-4, identifies the multiple IPCs needed by this subsystem. The following subsections address these interfaces.

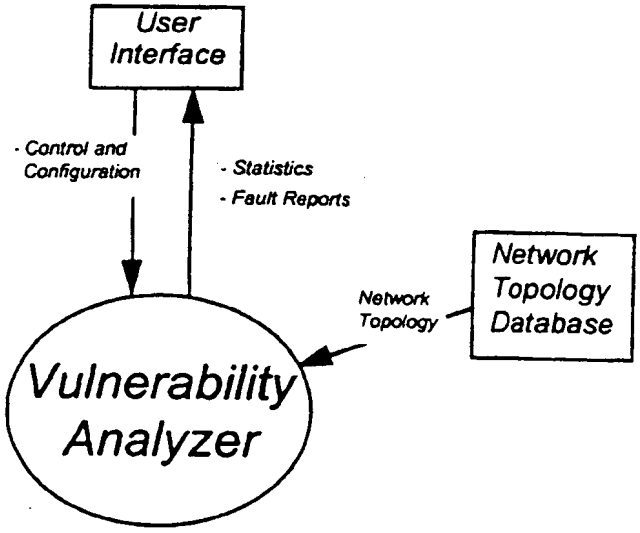


Figure 4-4 - Vulnerability Analyzer Context Diagram

4.2.1 User Interface

The User Interface is the mechanism used for control and receive analysis results for display.

4.2.1.1 Control and configuration

In response to a control message from the GUI subsystem, the Vulnerability Analyzer accepts the following information from the GUI message queue for configuration and control:

a) START operation
b) STOP operation
c) PAUSE operation

d) Send Status/Statistic data
e) Threshold and parameter values for algorithms

4.2.1.2 Analysis Results

Upon completion of the vulnerability analysis, the textual results file is displayed to the user in a scrollable window. The POTS case lists the critical node(s) followed by the most vulnerable links to that node. The AIN case also indicates the Most Critical SCP.

4.2.2 Network Topology Database

The Network Topology Database provides the Vulnerability Analyzer algorithms with the required relevant infrastructure data of the SS7 network. In addition to the topology data required by the Intrusion Detector, the Vulnerability Analyzer requires many additional attributes assigned to the nodes and links.

Routing in the GTE network for local STPs to regional STPs changes depending on the AIN service being accessed . This data had to be derived from drawings of the network topology and required manual analysis and database algorithms to derive the proper link routes.

5. Network Topology Database

The Network Topology Database is the persistent storage for the GTE SS7 network infrastructure. It contains all the nodal and link information required to implement both the Intrusion Detector and the Vulnerability Analyzer processes.

5.1 Concept of Execution

In response to a client process, the database provides the means, first, of determining the data set being requested by the client, and second, to send the data set to the proper process input message queue.

5.1.1 Interfaces

The context diagram, shown in Figure 5-5, identifies the multiple interfaces used by this subsystem. The following subsections address these interfaces.

APPENDIX A
SYSTEM OVERVIEW

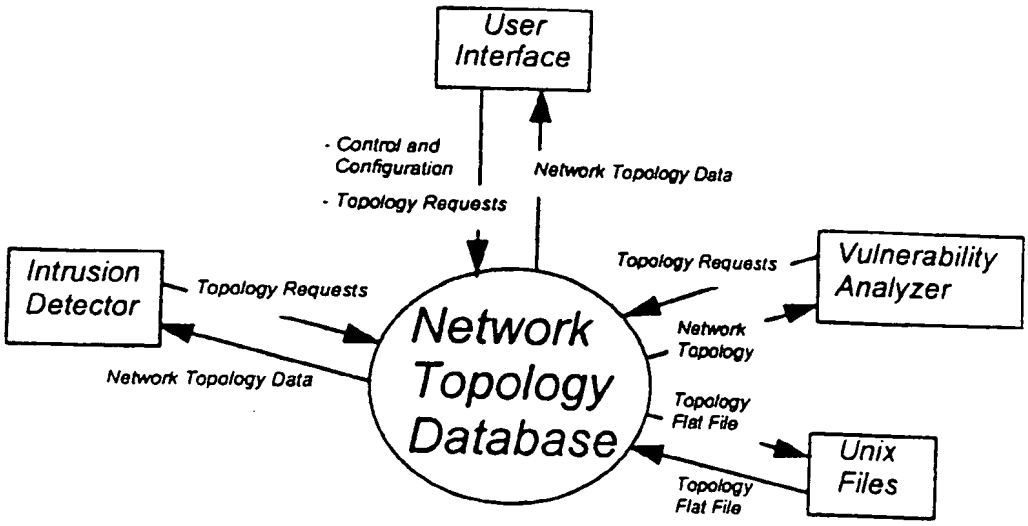


Figure 5-5 - Network Topology Database Domain Diagram

5.1.1.1 GUI/Intrusion Detector

The GUI and the Intrusion Detector will use the same information set from the database. The GUI extracts the information needed to construct the operator's view of the local SS7 network, used to display the real-time conclusions of the Intrusion Detector. The Intrusion Detector uses the link-node relationships to accomplish its algorithms (e.g., determine nearest neighbor, etc.).

5.1.1.2 Vulnerability Analyzer

The Vulnerability Analyzer requires a different information set from the of the Intrusion Detector. It's requirements include not only link-node relationships, but also, link media type, mode supplier, SS7 services provided and so on.

APPENDIX B
SOFTWARE USER'S MANUAL

TABLE OF CONTENTS

APPENDIX B
SOFTWARE USER'S MANUAL

TABLE OF CONTENTS

APPENDIX B
SOFTWARE USER'S MANUAL

LIST OF FIGURES

APPENDIX B
SOFTWARE USER'S MANUAL

LIST OF TABLES

APPENDIX B
SOFTWARE USER'S MANUAL

1. Scope

1.1 System Overview

The System Network and Signal Infrastructure Vulnerability Analysis and Intrusion Detection System (hereafter referred to as the system) is a software application capable of providing real-time protection to the U.S. telecommunications Signaling System No. 7 (SS7) infrastructure.

The goal of the system is to perform the following:

a) Determine the vulnerability of the SS7 network based on its topology and identify the network elements most vulnerable to intrusion.
b) Detect intrusions to SS7 links being monitored.
c) Provide a User Interface for operator control and status display in support of the above processes.

The system uses a Sun Microsystems's SPARC-20 platform, running the Solaris 2.5 operating system.

1.2 Document Overview

This Software Users Manual (SUM) describes the procedures required for using the System prototype. This system software includes two (2) independent tools:

a) Intrusion Detector (including SS7 Monitoring, User Interface, and Anomaly Detection processes)
b) Vulnerability Analyzer (User Interface, and Vulnerability Analysis processes)

2. References

The documents identified below provide background information and are incorporated herein by reference.

	DOCUMENT No.	TITLE
[1]	ISO 9001	International Organization of Standards 9001
[2]	ANSI T1.111-1996	Signaling System Number 7, Message Transfer Part (MTP), American National Standards Institute Inc., 1996
[3]	ANSI T1.112-1996	Signaling System Number 7, Signaling Connection Control Part (SCCP), American National Standards Institute Inc., 1996
[4]	ANSI T1.113-1995	Signaling System Number 7, Integrated Services Digital Network User Part (ISDN), American National Standards Institute Inc., 1995

3. (U) System Requirements

This section describes the workstation' s configuration and system requirements necessary for the System prototype. These requirements are shown below:

Table 3-1 - System Requirements

Name	Description
PLATFORM	
Operating System	Solaris Version 2.5

APPENDIX B
SOFTWARE USER'S MANUAL

Name		Description
PLATFORM		
	System RAM	64Meg or greater
COTS Software		
	Sybase Server	Version 10.02
	Sybase Open Client	Version 11.1
	ICS OSF/Motif	Version 1.2.4

4. System Installation and Environment Setup

This section describes the installation and environment setup procedures necessary to get started with the application. The following steps are required to run the system:

a) Modify the environment by adding the following lines to your .cshrc file. After modification, perform the required **source .cshrc** to implement these changes.

i) **setenv SYSTEMHOME** ***pathname***, **where** *pathname* defines the path of the System home directory.
ii) **setenv INTR_CONFIG** $(SYSTEMHOME)/config, **where** $(SYSTEMHOME)/config defines the path of the System configuration sub-directory.
iii) **setenv XENVIRONMENT** $INTR_CONFIG/gui.res, **where** $INTR_CONFIG/gui.res defines the configuration file used for the X window environment.
iv) **setenv MOTIFHOME** /opt/Motif124/usr, **where** *pathname* defines the path of the Motif compile-time libraries directory.
v) **setenv SYBASE** ***pathname***, **where** *pathname* defines the path of the Sybase database utilities (/cots/sybase)
vi) **setenv DSQUERY** SYSTEM
vii) **setenv LD_LIBRARY_PATH** ${LD_LIBRARY_PATH}:$MOTIFHOME/lib/X11:/usr/lib/X11::usr/lang/lib:.usr/lib:$OPENWINHOME/lib::$OPENWINHOME/lib:/usr/lib:$MOTIFHOME/lib/X11:/usr/dt/lib
viii) **setenv PATH** ${PATH}:$SYBASE/bin

b) **INSTALLATION:** Move to this directory and extract TAR format tape:

a) **mkdir** ***pathname***, **where** *pathname* defines the path of the System home directory (as defined by **SYSTEMHOME**).
b) **cd $SYSTEMHOME**, to move to this directory for installation.
c) **tar xvf /dev/rmt/0**, to extract the tar file to the current directory.

5. (U) Intrusion Detector Execution Procedure

This section describes the information and instructions necessary for user interaction with the system Intrusion Detector. It gives the step-by-step procedures for executing the software and identifies the options available to the user.

APPENDIX B
SOFTWARE USER'S MANUAL

5.1 Initialization and Startup

This section describes the initialization and startup procedures necessary to execute the software. To launch the Intrusion Detector executable, type IntrusionDetector on the command line of your UNIX shell. Upon startup of the System's Intrusion Detector application, the following events are performed:

a) The required environment variables are retrieved from the system. These variables are defined in section 4.

b) The application retrieves its default configuration from the startup initialization file "init_config.intr". This file is stored in the directory **SYSTEMHOME/config**.

Once the initialization of the application has completed, its GUI is displayed and ready for user interaction. The user must configure the tool, via the menu options or loading a previously saved configuration file.

5.2 User Inputs and Control

The following sections describe the user inputs and control for the system software. On-line help is provided within the application via the Help option. The user's primary control is in the form of a Graphical User Interface (GUI) shown in Figure 5-1. The GUI is provided to service the following operator control.

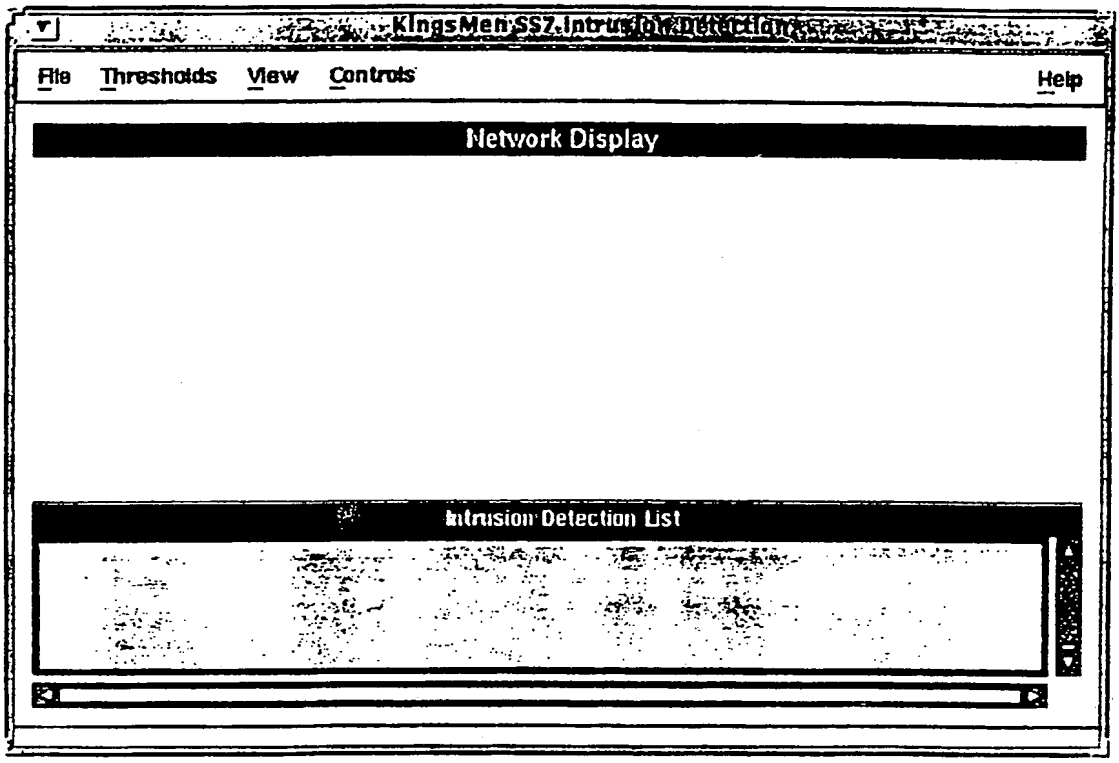


Figure 5-1- Top-Level GUI Environment

5.2.1 File Management

The application provides the capability to save and retrieve both configuration and output log files via the GUI.

APPENDIX B
SOFTWARE USER'S MANUAL

5.2.2 Threshold Management

The application provides the capability to view and modify all adjustable parameters required by the intrusion detection algorithms for maximum flexibility and expansion. The following list describes each of these GUI adjustable parameters.

Table 5-1 - Intrusion Detection Adjustable Parameters

Threshold Name	Description
Max Number of Changeovers	The threshold for number of MTPCHANGEOVER messages per a predefined time period.
Max Number of Emergency Changeovers	The threshold for number of MTP EMERGENCY CHANGEOVER messages per a predefined time period.
Max Number of Node Transfer Prohibit	The threshold for number of MTP Node TRANSFER PROHIBIT messages per a predefined time period.
Max Number of Cluster Transfer Prohibit	The threshold for number of MTP Cluster TRANSFER PROHIBIT messages per a predefined time period.
Max Number of Node Transfer Restrict	The threshold for number of MTP Node TRANSFER RESTRICT messages per a predefined time period.
Max Number of Cluster Transfer Restrict	The threshold for number of MTP Cluster TRANSFER RESTRICT messages per a predefined time period.
Max Number of Node Transfer Control	The threshold for number of MTP Node TRANSFER CONTROL messages per a predefined time period.
Max Number of Cluster Transfer Control	The threshold for number of MTP Cluster TRANSFER CONTROL messages per a predefined time period.
Max Number of Link Inhibits	The threshold for number of MTP LINK INHIBIT messages per a predefined time period.
Max Number of Pattern SLC	The threshold for number of consecutive SLCs inhibited, prohibited, restricted, or reset.
Max Number of Node Releases	The threshold for number of ISUP Node RELEASE messages per a predefined time period.
Max Number of Group Releases	The threshold for number of ISUP GROUP RELEASE messages per a predefined time period.
Max Number of Node Resets	The threshold for number of ISUP Node RESET messages per a predefined time period.
Max Number of Group Resets	The threshold for number of ISUP GROUP RESET messages per a predefined time period.
Max Number of Node Blocks	The threshold for number of ISUP Node BLOCK messages per a predefined time period.
Max Number of Group Blocks	The threshold for number of ISUP GROUP BLOCK messages per a predefined time period.
Max Number of Unequipped Circuits	The threshold for number of ISUP ISUP UNEQUIPPED CIRCUIT messages per a predefined time period.
Max Number of Circuits Query	The threshold for number of ISUP ISUP CIRCUIT QUERIES messages per a predefined time period.
Max Number of Pattern CIC	The threshold for number of consecutive CICs released, blocked, reset or unequipped.
Max Number of Signaling Route Set Test Anomalies	The threshold for number of ISUP SIGNALING ROUTE SET TEST anomalies per a predefined time period.
Max Number of Signaling Route Set Congestion Test Anomalies	The threshold for number of ISUP SIGNALING ROUTE SET CONGESTION TEST anomalies per a predefined time period.

APPENDIX B
SOFTWARE USER'S MANUAL

Threshold Name	Description

5.2.3 View Control

The application provides the capability to enter monitor point(s) to which the protocol analyzer is connected. This data is used to define the local topology view displayed to the user. The monitor points are entered using the "View | Monitor Point Selection" menu option provided by the GUI.

5.2.4 Start/Stop

The application provides the capability to start and stop processing of the application using the "Control Start" and the "Control | Stop" GUI menu options, respectively.

In order to start execution, valid monitoring points must be loaded, either from the GUI or by loading a previously stored configuration file. An error is displayed if this condition is not met. The generation and display of the local topology view immediately follows.

5.2.5 Termination

The application provides the capability to terminate execution of the application using the "File : Exit" menu option provided by the GUI.

5.3 System Inputs

The following sections describe the system inputs to the system and are required for the proper operation of the application.

5.3.1 Protocol Analyzer

The protocol analyzer selected for the system is the INET Turbo-7 protocol analyzer. Up to four (4) SS7 links can be monitored at one time by this device. The message format, shown in Table 5-2, is expected from the analyzer via the TCP/IP port.

Table 5-2 - INET MSU Record Format

Field Name	Number of Bytes	Description
Timestamp	4	GMT
Tick	2	millisecond resolution
Port Number	1	Analyzer's Port Number used for monitoring (Spinode Link Number)
Length	2	Length of the remainder of this record (to the end)
MSU Body	X	Forwarded message

5.3.2 Input MSU Test File

This section describes the MSU formats used by the input test file. The test file injects the test MSU into the real-time path for the purpose of diagnostics. Table 5-3 details the different formats expected for the different SS7 MSU types.

Table 5-3 - Input Test File MSU Formats

MSU Type	MSU Function	MSU Data Fields	Comments

APPENDIX B
SOFTWARE USER'S MANUAL

MSU Type MTP	MSU Function	MSU Data Fields	Comments
		Monitored Port Number	INET Port number assigned to desired link
		Direction	Directional indication (0/1 = DTE/DCE)
		delta Time Stamp	Time delay of MSU insertion
		MSU Type	Indicates whether MTP (0) or ISUP (5)
		MSU function	MSU function (See reference [2])
		OPC	Origination Point Code of MSU
		DPC	Designation Point Code of MSU
		SLC	Signal Link Code of MSU
		destination (for TFP, TFR, TFA only)	Destination Point Code of Transfer Control MSUs
ISUP			
	Address Complete Answer Message Call Progress Unequipped Circuit Release Complete CIC Reset CIC UnBlock CIC UnBlock Ack CIC Block CIC Block Ack	Monitored Port Number	INET Port number assigned to desired link
		Direction	Directional indication (0/1 = DTE/DCE)
		delta Time Stamp	Time delay of MSU insertion
		MSU Type	Indicates whether MTP (0) or ISUP (5)
		MSU function	MSU function (See reference [4])
		OPC	Origination Point Code of MSU
		DPC	Designation Point Code of MSU
		CIC	Circuit Identification Code
	Release Requested	Monitored Port Number	INET Port number assigned to desired link
		Direction	Directional indication (0/1 = DTE/DCE)
		delta Time Stamp	Time delay of MSU insertion
		MSU Type	Indicates whether MTP (0) or ISUP (5)
		MSU function	MSU function (See reference [4])
		OPC	Origination Point Code of MSU
		DPC	Designation Point Code of MSU
		CIC	Circuit Identification Code
		Cause Code	Cause Code of RELEASE MSU
	Initial Address	Monitored Port Number	INET Port number assigned to desired link
		Direction	Directional indication (0/1 = DTE/DCE)
		delta Time Stamp	Time delay of MSU insertion
		MSU Type	Indicates whether MTP (0) or ISUP (5)
		MSU function	MSU function (See reference [4])
		OPC	Origination Point Code of MSU
		DPC	Designation Point Code of MSU
		CIC	Circuit Identification Code
		Called Area Code	
		Called Number	
		Calling Area Code	
		Calling Number	
	Group Reset Group Block Group Block Ack Group UnBlock Group UnBlock Ack	Monitored Port Number	INET Port number assigned to desired link
		Direction	Directional indication (0/1 = DTE/DCE)
		delta Time Stamp	Time delay of MSU insertion
		MSU Type	Indicates whether MTP (0) or ISUP (5)
		MSU function	MSU function (See reference [4])

NOT FURNISHED UPON FILING

NO PRESENTADO(A) EN EL MOMENTO DE LA PRESENTACIÓN

NON SOUMIS(E) AU MOMENT DU DÉPÔT

APPENDIX B
SOFTWARE USER'S MANUAL

occurrence of an anomaly, the event and background information is logged and stored in the Intrusion Detection log.

Table 5-4 - Output Anomaly Messages

Anomaly Code	Description of Anomaly	SS7 Protocol Effected
100	LINK NEAREST NEIGHBOR FAILURE - A SS7 MTP message was received where the OPC and DPC did not correspond to the required link.	MTP
101	EXCESSIVE CHANGEOVER - The occurrences of CHANGEOVER messages to a link exceeded the operator's adjustable threshold.	MTP
102	EXCESSIVE EMERGENCY CHANGEOVER - The occurrences of EMERGENCY CHANGEOVER messages to a link exceeded the operator's adjustable threshold.	MTP
103	CHANGEOVER REQUEST TIMEOUT - A timeout has been detected after a CHANGEOVER message was detected on a monitored link. NO corresponding acknowledgment was detected.	MTP
104	EXCESSIVE NODE TRANSFER PROHIBITS - The occurrences of node TRANSFER PROHIBIT messages to a link exceeded the operator's adjustable threshold.	MTP
105	EXCESSIVE CLUSTER TRANSFER PROHIBITS - The occurrences of cluster TRANSFER PROHIBIT messages to a link exceeded the operator's adjustable threshold.	MTP
106	EXCESSIVE NODE TRANSFER RESTRICTS - The occurrences of node TRANSFER RESTRICT messages to a link exceeded the operator's adjustable threshold.	MTP
107	EXCESSIVE CLUSTER TRANSFER RESTRICTS - The occurrences of cluster TRANSFER RESTRICT messages to a link exceeded the operator's adjustable threshold.	MTP
108	EXCESSIVE NODE TRANSFER CONTROL - The occurrences of node TRANSFER CONTROL messages to a link exceeded the operator's adjustable threshold.	MTP
109	EXCESSIVE CLUSTER TRANSFER CONTROL - The occurrences of cluster TRANSFER CONTROL messages to a link exceeded the operator's adjustable threshold.	MTP
110	EXCESSIVE LINK INHIBITS - The occurrences of node LINK INHIBIT messages to a link exceeded the operator's adjustable threshold.	MTP
111	INVALID SLC INHIBIT PATTERN - The pattern of inhibit SLCs observed on a link was not random and exceeded the operator's adjustable threshold.	MTP
112	INVALID CHANGEOVER - A CHANGEOVER message was received while the same monitored link was already in a CHANGEOVER state.	
113	INVALID CHANGEOVER ACKNOWLEDGE - A CHANGEOVER message was received with NO corresponding CHANGEOVER message detected on the same monitored link.	MTP
114	INVALID DIRECTION ON CHANGEOVER ACKNOWLEDGE - A CHANGEOVER ACKNOWLEDGE message was received from the wrong direction relative to the last corresponding MSU message.	MTP
115	INVALID EMERGENCY CHANGEOVER - An EMERGENCY CHANGEOVER message was received while the same monitored link was already in a CHANGEOVER state.	
116	INVALID EMERGENCY CHANGEOVER ACKNOWLEDGE - An EMERGENCY CHANGEOVER message was received with NO corresponding CHANGEOVER message detected on the same monitored link.	MTP
117	INVALID DIRECTION ON EMERGENCY CHANGEOVER ACKNOWLEDGE - An	MTP

APPENDIX B
SOFTWARE USER'S MANUAL

Anomaly Code	Description of Anomaly	SS7 Protocol Effected
	EMERGENCY CHANGEOVER ACKNOWLEDGE message was received from the wrong direction relative to the last corresponding MSU message.	
118	INVALID OPC ON TRANSFER PROHIBIT- A TRANSFER PROHIBIT message was received originating from a point code and did not correspond to a STP point code.	MTP
119	INVALID LOCAL TRANSFER PROHIBIT- A TRANSFER PROHIBIT message was received with NO corresponding CHANGEOVER or LINK INHIBIT detected on the monitored link to the destination point code.	MTP
120	INVALID REMOTE TRANSFER PROHIBIT- A TRANSFER PROHIBIT message was received with NO corresponding TRANSFER PROHIBIT detected from a connecting STP.	MTP
121	INVALID OPC ON TRANSFER RESTRICT - A TRANSFER RESTRICT message was received originating from a point code and did not correspond to a STP point code.	MTP
122	INVALID LOCAL TRANSFER RESTRICT - A TRANSFER RESTRICT message was received with NO corresponding CHANGEOVER or LINK INHIBIT detected on the monitored link to the destination point code.	MTP
123	INVALID REMOTE TRANSFER RESTRICT - A TRANSFER RESTRICT message was received with NO corresponding TRANSFER PROHIBIT detected from a connecting STP.	MTP
124	INVALID SIGNALING ROUTE SET TEST- A SIGNALING ROUTE SET TEST message was received with NO corresponding TRANSFER PROHIBIT or TRANSFER RESTRICT detected on the same monitored link.	MTP
125	INVALID NUMBER OF SIGNALING ROUTE SET TESTS PROHIBIT to TFA - Less than two (2) SIGNALING ROUTE SET TEST PROHIBIT messages were received before a corresponding TRANSFER ALLOW message was detected on the same monitored link.	MTP
126	INVALID NUMBER OF SIGNALING ROUTE SET TESTS RESTRICT to TFA - Less than two (2) SIGNALING ROUTE SET TEST RESTRICT messages were received before a corresponding TRANSFER ALLOW message was detected on the same monitored link.	MTP
127	INVALID TRANSFER ALLOWED - A TRANSFER ALLOWED message was received with NO corresponding SIGNALING ROUTE SET TEST message detected on the same monitored link.	MTP
128	INVALID DIRECTION ON TRANSFER ALLOWED - A TRANSFER ALLOWED message was received from the wrong direction relative to the last corresponding MSU message.	MTP
129	INVALID OPC ON TRANSFER CONTROL - A TRANSFER CONTROL message was received originating from a point code and did not correspond to a STP point code.	MTP
130	INVALID SIGNALING ROUTE SET CONGESTION TEST- A SIGNALING ROUTE SET CONGESTION TEST message was received with NO corresponding TRANSFER CONTROL detected on the same monitored link.	MTP
131	INVALID NUMBER OF SIGNALING ROUTE SET TESTS- Less than two (2) SIGNALING ROUTE SET TEST messages were received before a corresponding TRANSFER ALLOW message was detected on the same monitored link.	MTP
132	INVALID LINK INHIBIT - A LINK INHIBIT message was detected on a monitored link that was tagged NOT AVAILABLE or LINK INHIBIT was DISABLED.	MTP
133	INVALID NUMBER OF LINK INHIBITS - Greater than two (2) LINK INHIBIT messages were detected on the same monitored link.	MTP
134	LINK INHIBIT REQUEST TIMEOUT - A T14 timeout has been detected after a LINK	MTP

APPENDIX B
SOFTWARE USER'S MANUAL

Anomaly Code	Description of Anomaly	SS7 Protocol Effected
	INHIBIT message was detected on a monitored link. NO corresponding acknowledgment or denial was detected.	
135	INVALID LINK INHIBIT ACKNOWLEDGE - A LINK INHIBIT ACKNOWLEDGE message was received with NO corresponding LINK INHIBIT message detected on the same monitored link.	MTP
136	LINK INHIBIT ACKNOWLEDGE TIMEOUT - A MAX(T20,T21) timeout has been detected after a LINK INHIBIT ACKNOWLEDGE message was detected on a monitored link. NO corresponding TEST or UNINHIBIT was detected.	MTP
137	INVALID LINK LOCAL TEST - A LINK LOCAL TEST message was received with NO corresponding LINK INHIBIT ACKNOWLEDGE message detected on the same monitored link.	MTP
138	INVALID NUMBER OF LINK LOCAL TESTS- Less than two (2) consecutive LINK LOCAL TEST messages were received before a corresponding LINK UNINHIBIT or LINK FORCED UNINHIBIT message was detected on the same monitored link.	MTP
139	LINK LOCAL TEST TIMEOUT - A T20 timeout has been detected after a LINK LOCAL TEST message was detected on a monitored link. NO corresponding LINK UNINHIBIT or LINK FORCED UNINHIBIT message was detected.	MTP
140	INVALID LINK REMOTE TEST - A LINK REMOTE TEST message was received with NO corresponding LINK INHIBIT ACKNOWLEDGE message detected on the same monitored link.	MTP
141	INVALID NUMBER OF LINK REMOTE TESTS- Less than two (2) consecutive LINK REMOTE TEST messages were received before a corresponding LINK UNINHIBIT or LINK FORCED UNINHIBIT message was detected on the same monitored link.	MTP
142	LINK REMOTE TEST TIMEOUT - A T21 timeout has been detected after a LINK REMOTE TEST message was detected on a monitored link. NO corresponding LINK UNINHIBIT or LINK FORCED UNINHIBIT message was detected.	MTP
143	RESERVED	MTP
200	EXCESSIVE RELEASES - The occurrences of CIC RELEASE messages exceeded the operator's adjustable threshold.	ISUP
201	EXCESSIVE GROUP RESETS - The occurrences of CIC GROUP RESET messages exceeded the operator's adjustable threshold.	ISUP
202	EXCESSIVE NODE RESETS - The occurrences of CIC NODE RESET messages exceeded the operator's adjustable threshold.	ISUP
203	EXCESSIVE GROUP BLOCKS - The occurrences of CIC GROUP BLOCK messages exceeded the operator's adjustable threshold.	ISUP
204	EXCESSIVE NODE BLOCKS - The occurrences of CIC NODE BLOCK messages exceeded the operator's adjustable threshold.	ISUP
205	EXCESSIVE UNEQUIPPED CIRCUITS - The occurrences of CIC UNEQUIPPED CIRCUIT messages exceeded the operator's adjustable threshold.	ISUP
206	EXCESSIVE CIRCUIT QUERIES - The occurrences of CIC CIRCUIT QUERY messages exceeded the operator's adjustable threshold.	ISUP
207	INVALID CIC RELEASE PATTERN - The pattern of released CICs observed was not random and exceeded the operator's adjustable threshold.	ISUP
208	INVALID CIC BLOCK PATTERN - The pattern of blocked CICs observed was not random and exceeded the operator's adjustable threshold.	ISUP
209	INVALID CIC RESET PATTERN - The pattern of reset CICs observed was not	ISUP

APPENDIX B
SOFTWARE USER'S MANUAL

Anomaly Code	Description of Anomaly	SS7 Protocol Effected
	random and exceeded the operator's adjustable threshold.	
210	INVALID CIC UNEQUIPPED PATTERN - The pattern of unequipped CICs observed was not random and exceeded the operator's adjustable threshold.	ISUP
211	INVAILD ADDRESS COMPLETE - An ADDRESS COMPLETE message was received with NO corresponding INITIAL ADDRESS message detected on the same or mated monitored link.	ISUP
212	INVALID POINT CODE - A SS7 MSU message was received with an invalid point code (OPC or DPC).	ISUP
213	TRUNK NEAREST NEIGHBOR FAILURE - A SS7 ISUP message was received where the OPC and DPC did not correspond to nodes with a common trunk.	ISUP
214	INVALID INITIATED CALL - An INITIAL ADDRESS message was received for a CIC already allocated. This MSU has been ignored by the network.	ISUP
215	INVALID RELEASE - A RELEASE message was received with NO corresponding INITIAL ADDRESS or ADDRESS COMPLETE message detected in the opposite direction on the same or mated monitored link.	ISUP
216	ABNORMAL CAUSE CODE ON RELEASE - A valid RELEASE message was received with an abnormal CAUSE CODE.	ISUP
217	RELEASE TIMEOUT - A five (5) minute timeout has been detected after a RELEASE message was detected on a monitored link. NO corresponding RELEASE COMPLETE message detected in the opposite direction on the same or mated monitored link.	ISUP
218	INVALID RELEASE COMPLETE - A RELEASE COMPLETE was received with a corresponding BLOCK message detected on the same or mated monitored link, however, the direction of the RLC message, relative to the corresponding BLOCK message, was incorrect.	ISUP
219	INVALID RELEASE COMPLETE - A RELEASE COMPLETE message was received with NO corresponding RELEASE, RESET or BLOCK message detected on the same or mated monitored link.	ISUP
220	INVALID DIRECTION RELEASE COMPLETE - A RELEASE COMPLETE was received from the wrong direction relative to the last corresponding MSU message.	ISUP
221	INSERTED RESET - A RELEASE COMPLETE message was correlated to a previously detected BLOCK message in the same direction on the same or mated monitored link. This indicates a RESET message inserted at OPC.	ISUP
222	INVALID GROUP RESET - A two (2) consecutive GROUP RESET messages were not in the same direction on the same or mated monitored link.	ISUP
223	GROUP RESET TIMEOUT - A five (5) second timeout for the second of two GROUP RESET messages has occurred.	ISUP
224	INVALID RESET - A RESET message was received and was correlated to a previously detected RELEASE COMPLETE message in the opposite direction on the same or mated monitored link.	ISUP
225	RESET TIMEOUT - A fifteen (15) second timeout has occurred between a RESET message and its corresponding UNEQUIPPED CIRCUIT message on the same or mated monitored link.	ISUP
226	INVALID GROUP BLOCK - A two (2) consecutive GROUP BLOCK messages were not in the same direction on the same or mated monitored link.	ISUP
227	GROUP BLOCK TIMEOUT - A five (5) second timeout for the second of two (2) GROUP BLOCK messages has occurred.	ISUP
228	INVALID BLOCK - A BLOCK message was received and was correlated to a previously detected UNBLOCK ACKNOWLEDGE message in the opposite direction	ISUP

APPENDIX B
SOFTWARE USER'S MANUAL

Anomaly Code	Description of Anomaly	SS7 Protocol Effected
	on the same or mated monitored link within a fifteen (15) second time internal.	
229	INVALID BLOCK ACKNOWLEDGE - A BLOCK ACKNOWLEDGE message was received with NO corresponding BLOCK message detected in the opposite direction on the same or mated monitored link.	ISUP
230	INVALID DIRECTION BLOCK ACKNOWLEDGE - A BLOCK ACKNOWLEDGE was received from the wrong direction relative to the last corresponding MSU message.	ISUP
231	BLOCK ACKNOWLEDGE TIMEOUT - A five (5) minute timeout has been detected after a BLOCK ACKNOWLEDGE message was received on a the same or mated monitored link. NO corresponding UNBLOCK message was detected.	ISUP
232	INVALID UNBLOCK - A UNBLOCK message was received with NO corresponding BLOCK ACKNOWLEDGE message detected in the opposite direction on the same or mated monitored link.	ISUP
233	EARLY UNBLOCK - A UNBLOCK message was received and was correlated to a previously detected BLOCK ACKNOWLEDGE message in the opposite direction on the same or mated monitored link within a fifteen (15) second time internal.	ISUP
234	INVALID DIRECTION FOR UNBLOCK - A UNBLOCK was received from the wrong direction relative to the last corresponding MSU message.	ISUP
235	INVALID UNBLOCK ACKNOWLEDGE - A UNBLOCK ACKNOWLEDGE message was received with NO corresponding UNBLOCK message detected in the opposite direction on the same or mated monitored link.	ISUP
236	INVALID DIRECTION FOR UNBLOCK ACKNOWLEDGE - A UNBLOCK ACKNOWLEDGE was received from the wrong direction relative to the last corresponding MSU message.	ISUP
237	INVALID UNEQUIPPED CIRCUIT - An UNEQUIPPED CIRCUIT message was received with NO corresponding RELEASE, RESET, GROUP RESET, GROUP BLOCK or BLOCK message detected in the opposite direction on the same or mated monitored link.	ISUP
238	INVALID DIRECTION FOR UNEQUIPPED CIRCUIT - An UNEQUIPPED CIRCUIT message was received from the wrong direction relative to the last corresponding MSU message.	ISUP
239	INVALID CIRCUIT QUERY- A CIRCUIT QUERY message was received and was correlated to a previously detected RELEASE COMPLETE message in the opposite direction on the same or mated monitored link.	ISUP
240 - 299	Reserved	

5.4.3 (U) Operational Error and Warning Messages

This section identifies all error messages output by the system, the meaning of each error message, and the action to be taken when each message appears. These messages are displayed to the user via the GUI. In addition, faults are logged by the each individual process into its corresponding flat file. Each fault log can be enabled/disabled by the system configuration file previously loaded.

Table 5-5 - Operational Error and Warning Messages

Error Code	Description of Error/Warning	Action Required
1000	ERROR: CHILD CREATION FAULT DETECTED - There was a	Verify the presence of the

APPENDIX B
SOFTWARE USER'S MANUAL

Error Code	Description of Error/Warning	Action Required
	failure during the creation of a child process (Process Manager).	corresponding executable and restart the Intrusion Detector.
1001	ERROR: EXCESSIVE ANOMALIES DETECTED - The number of anomalies have exceeded the system limit (Intrusion Detection Process).	Adjust thresholds, exit and restart the Intrusion Detector tool.
1002	ERROR: INVALID MONITOR POINT LOADED - A monitor point's point code or link ID is invalid (Display Management).	Enter valid monitor point as prompted by the GUI.
1003	ERROR: DUPLICATE MONITOR POINT LOADED - The monitor point entry entered already exists.	Enter valid monitor point as prompted by the GUI.
1004	ERROR: INVALID PORT NUMBER DETECTED - A port number was detected that does not correspond to an existing monitor point entry. MSU was ignored (Intrusion Detection Process).	Enter valid port number as prompted by the GUI.
1005	ERROR: INVALID FILENAME - The filename entered was not found (Display Management).	Enter valid filename as prompted by the GUI
1006	ERROR: UNDEFINED ENVIRONMENT VARIABLE - An environment variable has not been defined -- Aborting program (All processes).	Terminate program, define environment variable and restart program.
1007	ERROR: UNEXPECTED CHILD PROCESS TERMINATION - An unexpected termination of a child process has been detected – Aborting program (Display Management).	Restart program.
1008	ERROR: IPC SEND ERROR - Message Queue SEND Error detected – Aborting program (All processes).	
1009	ERROR: IPC OPEN ERROR - Message Queue OPEN Error detected – Aborting program (All processes).	
1010	ERROR: COMM PORT OPEN FAILURE - The Communication Port failed during an open attempt (Data Collector Process).	Verify socket connection between the protocol analyzer and the System workstation.
1011	ERROR: BAD TEST FILE DATA - Invalid data format within test input file specified (Data Collector Process).	Verify test file name selected under the "Input Selection" menu.
1012	ERROR: DATABASE FAILURE - Database communication problem. Unable to connect to database server -- Aborting program (All processes).	Verify database configuration.
1013 to 1099	Reserved	
1100	WARNING: TRANSFER PROHIBIT IS UNVERIFIABLE - A TRANSFER PROHIBIT message was received that could not be verified due to the monitoring point set selection (Intrusion Detection Process).	No Action Required.
1101	WARNING: TRANSFER RESTRICT IS UNVERIFIABLE - A TRANSFER RESTRICT message was received that could not be verified due to the monitoring point set selection (Intrusion Detection Process).	No Action Required.
1102	WARNING: TRANSFER CONTROL IS UNVERIFIABLE - A TRANSFER CONTROL message was received that could not be verified due to the monitoring point set selection (Intrusion Detection Process).	No Action Required.
1103	WARNING: MTP INTRUSION DETECTION ONLY - Due to the	Enter new monitor points that

APPENDIX B
SOFTWARE USER'S MANUAL

Error Code	Description of Error/Warning	Action Required
	monitoring point set selected, only MTP intrusion detection is available (Intrusion Detection Process).	monitor all links to a desired SSP for ISUP.
1104	WARNING: PARTIAL CONFIGURATION LOADED - An incomplete configuration file was loaded (Display Management).	Load complete configuration file.
1105	WARNING: COMM PORT OPEN RETRY - No Communication Port connection – Retrying (Data Collector Process).	Verify socket connection between the protocol analyzer and the System workstation.
1106 to 1199	Reserved	

APPENDIX B
SOFTWARE USER'S MANUAL

6. (U) Vulnerability Analyzer Execution Procedure

This section describes the information and instructions necessary for user interaction with the System Vulnerability Analyzer. It gives the step-by-step procedures for executing the software and identifies the options available to the user.

6.1 Initialization and Startup

This section describes the initialization and startup procedures necessary to execute the software. To launch the Vulnerability Analyzer executable, type VulnerabilityAnalysis on the command line of your UNIX shell. Upon startup of the System's Vulnerability Analyzer application, the following events are performed:

a) The required environment variables are retrieved from the system. These variables are defined in section 4.

b) The application retrieves its default configuration from the startup initialization file "init_config.vuln". This file is stored in the directory **SYSTEMHOME/config**.

Once the initialization of the application has completed, its GUI is displayed and ready for user interaction. The user must configure the tool, via the menu options or loading a previously saved configuration file.

6.2 User Inputs and Control

The following sections describe the user inputs and control for this application. On-line help is provided within the application via the Help option. The user's primary control is in the form of a Graphical User Interface (GUI) shown in Figure 4.2. The GUI is provided to service the following operator control.

APPENDIX B
SOFTWARE USER'S MANUAL

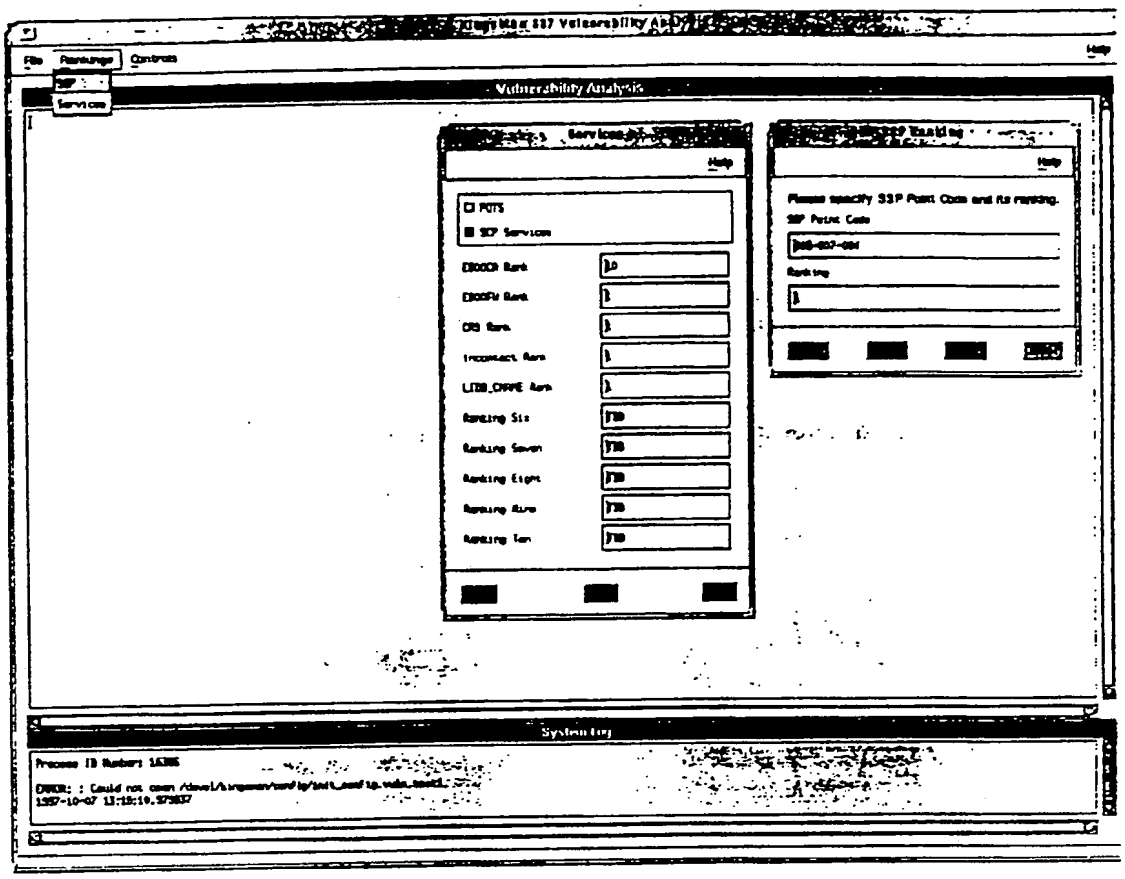


Figure 6-1 - Vulnerability Analysis Top Level GUI

6.2.1 File Management

The application provides the capability to save and retrieve both configuration and analysis result files via the GUI under the File selection.

6.2.1.1 File Save

The Save selection allows the user to save the current analysis results to a user specified file name. Also the user may select to save the current configuration to a user specified file name for later retrieval.

6.2.1.2 File Retrieve

The retrieve selection allows the user to retrieve an analysis results log or to retrieve an existing configuration file. When the Retrieve / Configuration is selected, the File window appears. The user may then enter a filter selection and click on the Filter button to narrow his selection, and click on a file name in the files section. The selected file is displayed under Selection and the user clicks on OK to load the file in memory. In order to view the loaded configuration file, the user must select Retrieve Analysis. Note that the file is not editable via the GUI. The parameters contained in the configuration file are described in Table 6-1.

Table 6-1 - Vulnerability Configuration Parameters

APPENDIX B
SOFTWARE USER'S MANUAL

Ranking Name	Description
POTS Service Rank	Priority ranking for POTS service
Physical Link Rank	Priority rankings for the physical media types of fiber, microwave, satellite, and coax.
Media Link Rank	The physical media provider rankings for GTE, AT&T, Sprint, MCI, Ameritech, Bell South, Southwestern Bell, Bell Atlantic, US West, Delta Communications, NTS Communications, PTI Communications, Norlite, and any others.
Functional Link Rank	Functional capacity rankings for the percent of utilization on the links and rankings based on the number of links in the linkset.
Security Link Rank	Rankings for the security characteristics of the link such as encryption, and the combination of point code screening (no point code screening, network only, network cluster, and network cluster member), with logic screening (no logic screening, message class, and message type).
Media Access Modifier	Multiplier applied to the media provider based on the link's physical media type of fiber, microwave, satellite, or coax.
Services Multi Modifier	Addend applied to the link score based on the number of services ranked at high, medium, and low rankings. High rank is from 8 to 10 inclusive, medium is from 4 to 7 inclusive, and low is from 1 to 3 inclusive.
Functional Capacity Modifier	Functional capacity subtrahend based on the utilization rank and the number of links rank, functional capacity addend based on the percent of traffic on the link which is generated internal, functional capacity addend based on the percent of traffic on the link which is generated external, the functional capacity subtrahend based on the score class and security monitoring, the security rank subtrahend based on the screening rank and security monitoring, and the service rank multiplier which is applied to the security rank.
Functional Capacity Limit	Functional capacity percent utilization lower and upper limits, the percent of traffic generated external lower and upper limits, and the threshold for the number of links in the linkset.
High Security Media Combo	Subtrahend applied to the link's physical access score when the link is classified as having high security, along with the various high, medium, and low combinations for functional services and functional capacity.
Medium Security Media Combo	Subtrahend applied to the link's physical access score when the link is classified as having medium security, along with the various high, medium, and low combinations for functional services and functional capacity.
Low Security Media Combo	Subtrahend applied to the link's physical access score when the link is classified as having low security, along with the various high, medium, and low combinations for functional services and functional capacity.
SSP Node Type Rank	Default node ranking for three types of SSPs: tandem, end office, and TOPS.
Overall Node Limits	Thresholds for the number of occupants located at the node
Overall Node Modifier	Node owner ranking for GTE, AT&T, MCI, Sprint, Bell Atlantic, Bell South, Pacific Bell, Ameritech, US West, LCI, and any others; addend applied to the criticality score based on the node access as far as occupied, remote public, or remote private; and the amount of reduction of the criticality score based on whether a security observation exists.
Correlation Modifier	The amount to reduce the link vulnerability score based on the number of hops the link is from the critical node.
Display Limit	The maximum number of nodes at the highest criticality score which may be identified as the most critical node. The maximum number of

APPENDIX B
SOFTWARE USER'S MANUAL

Ranking Name	Description
	links displaying detailed link information to the operator.
Network Area	Analyzed network regional area defined by longitude upper and lower bounds, and latitude upper and lower bounds.
Rank Assignment	SSP point codes and their associated SSP priority ranking.
Palletel Ranking	Services evaluated (POTS or SCP services). Priority rankings for the SCP services of E800CA, E800FW, CRS, INCONTACT, and LIDB CNAME.
Fault Log Configuration	Enabling or disabling of the fault log.

6.2.2 Rankings Management

The application provides the capability to view and modify the rankings of individual SSPs and services. Refer to Figure 4.2 to see the format of the windows. If the operator selects the SSP ranking then he must provide a SSP point code, and an integer ranking between one and ten inclusive. The SSP point code is of the format xxx-xxx-xxx, where x is an integer. If the user selects the services rankings then a Services window pops up with the default POTS service selected. If he changes the services selection to SCP Services, then he must supply an integer ranking between one and ten inclusive for each of the services identified in Table 6-2. By entering a high ranking for a service, the user is assigning a higher priority to the service for his analysis.

Table 6-2 - Vulnerability Adjustable Rankings

Service Ranking Name	Description
E800CA	800 service homed to California
E800FW	800 service homed to Indiana
CRS	Customer Routing Service for business customers (call forwarding)
INCONTACT	Customer Routing Service for residential customers
LIDB CNAME	Line Information Data Base Caller Name (calling card data, collect & third party billing, presubscribed interexchange carrier, foreign records, caller identification with names)

6.2.3 Controls

The application provides the user with the capability to start and stop processing of the application using the "Control Start" and the "Control | Stop" GUI menu options, respectively.

6.2.4 Termination

The application provides the capability to terminate execution of the application using the "File : Exit" menu option provided by the GUI (similar to the Intrusion Detection).

6.3 System Inputs

The following sections describe the system inputs to the system and are required for the proper operation of the application.

6.3.1 Topology Database

The topology database is the repository of information related to the configuration and the individual characteristics of each element of the GTE proprietary SS7 network.

6.3.2 Help Files

Several HELP flat files are required by the application in support of the HELP option within the GUI. These files must be installed at the path defined by the SYSTEMHELP environment variable (similar to the Intrusion Detector). The required help files are:

APPENDIX B
SOFTWARE USER'S MANUAL

a) file_help - This is the flat file containing the help text for the "File" menu options.
b) services_help - This is the flat file containing the help text for the "Rankings : Services" menu option.
c) vuln_monitor_help - This is the flat file containing the help text for the "Rankings : SSP" menu option.
d) vulnerability_help - This is the flat file containing the help text for the main Vulnerability Analysis menu.

6.4 Outputs

The following sections describe the expected outputs provided by the System Vulnerability Analyzer application.

6.4.1 Operator's Vulnerability Analysis Display and Analysis Log

The Vulnerability Analysis results are output to a log file and then displayed to the operator in a scrollable window. Both critical nodes and the most vulnerable links for attacking the critical nodes are recorded in the analysis output file and displayed to the user. The critical nodes are displayed in a descending order based on the score. Both the node criticality score and the link vulnerability score fall within the scale of one to ten inclusive. The following information is displayed in the log:

a) Critical SCP node point code and office name. Note that the critical SCP node is not applicable for POTS.
b) Number of critical nodes.
c) Critical node characteristics including the office name, point code, criticality score, and the raw criticality score.
d) Link information referenced to the critical node including the link identification, connecting node office names, and the vulnerability score.
e) Five most critical SSPs for each SSP type – tandem, end office, and telephone operator position service (TOPS).

6.4.2 (U) Operational Error and Warning Messages

The operational error and warning indications which are specific to the Vulnerability Analyzer, and displayed to the user via the GUI are described in Table 6-3. General System error messages in Table 5-5 which apply to the Vulnerability Analyzer are identified as either Process Manager or Display Management.

Table 6-3 - Vulnerability Operational Error and Warning Messages

Error / Warning Message	Description of Error/Warning	Action Required
Readjust SCP ranks	There is not a unique SCP identified as the most critical SCP because of the selected service rankings.	Adjust the Services Rankings and restart the Vulnerability Analyzer.
Too many critical nodes	The number of nodes identified as critical exceeds the node display limit in the configuration file.	On the command line of the UNIX shell, edit the configuration file that was loaded. Reload the modified file via File : Retrieve, and restart the Vulnerability Analyzer.
Database problem experienced	A problem occurred in trying to write the link vulnerability score to the database based on the number of hops that the link is from the critical node.	No action.
Message NOT sent to Vulnerability Analysis	Unsuccessful status returned when attempting to send a message to the Vulnerability Analysis process via the message queues.	Restart program.

APPENDIX B
SOFTWARE USER'S MANUAL

Error / Warning Message	Description of Error/Warning	Action Required
Cannot overwrite existing file	Selected filename is read-only.	Select another filename and resave.
Could not open <filename> file to display.	Error occurs if the selected configuration or analysis file cannot be retrieved, or if the user selects help and there is no help file.	Correct spelling of filename when prompted for filename to retrieve.
Monitoring point problem detected <SSP point code>	SSP point code specified is not in the database.	Under "Rankings : SSP", enter correct point code.
Could not open <filename>	Filename to be retrieved cannot be opened.	Check path name and filename spelling. Check file permissions.
Unknown field: <filename>. Must be Disabled or Enabled.	In configuration file the options for the fault log are either Disabled or Enabled.	On the command line of the UNIX shell, edit the configuration file and type either Disabled or Enabled for the fault log.
XENVIRONMENT not set. Needs to point to "gui.res" file.	Environment variable not set up correctly to point to the GUI's resource file.	Correct environment variable setup.

In addition, faults are logged by the Vulnerability Analysis process into its corresponding flat file with a default name of vulnerability_analyzer_class.log. The fault log can be enabled or disabled by the system configuration file previously loaded. Refer to Table 6-4 for a list of possible messages that may appear in the fault log.

Table 6-4 - Vulnerability Fault Log Messages

Error Message	Description of Error
Error writing SCP node criticality to database for <SCP point code>	Unable to write the specified SCP's criticality score to the database.
Error writing SSP node criticality to database for <SSP point code>	Unable to write the specified SSP's criticality score to the database.
Error writing STP node criticality to database for <STP point code>	Unable to write the specified STP's criticality score to the database.
Message Queue OPEN Error detected by Vulnerability – Aborting program.	Status is bad for either the Vulnerability incoming message queue or the Vulnerability outgoing message queue to the GUI.
Message Queue SEND Error detected from Vulnerability to Display Manager.	Error detected in trying to send a message to the Display Manager.
Node/link correlation not performed. Too many critical nodes identified. Critical node count is x. (x is an integer).	The number of identified critical nodes exceeds the node display limit specified in the configuration file.
Numerical error with STP <STP point code> net score denominator.	Identified STP would be a divide by zero as the number of hops to the critical SCP is zero.
Unable to initialize scores in database.	Call to database to initialize the node and link scores was unsuccessful.
Vulnerability is unable to get STP linksets.	The database was unable to return the linkset for the STP.
Vulnerability is unable to set net score for linkset <linkset name>	Error in trying to write the link score to the database for the specified linkset.

APPENDIX B
SOFTWARE USER'S MANUAL

7. (U) Notes

This section contains general information that aids in understanding this specification (e.g., background information, glossary).

7.1 (U) Abbreviations and Acronyms

All abbreviations and their meanings, as used in this document, are presented in the following alphabetical listing:

DPC	Designation Point Code
GMT	Greenwich Mean Time
GUI	Graphical User Interface
ISDN	Integrated Services Digital Network
ISUP	ISDN User Part
MTP	Message Transfer Part
OPC	Origination Point Code
POTS	Plain Old Telephone Service
SCP	Service Control Point
SS7	Signalling System 7
SSP	Service Switching Point
STP	Signalling Transfer Point
SUM	Software User's Manual

APPENDIX B
SOFTWARE USER'S MANUAL

(U) Topology Database Schema and Procedures
This section describes the information and instructions necessary for user setup and control of the Topology Database. The following is the step-by-step procedure required for use with the System prototype.

Prerequisites:

LOGIN: sa
PASSWORD: ""
Minimum size of tempdb database: 24MB
Data device named data_device_1
Index device named index_device_1

Run the following script to create the system_db database:

```
% $SYSTEMHOME/db/db_schema/system_db_init.sql
```

Run the following script to create the tables in the system_db database:

```
% $SYSTEMHOME/db/db_schema/create_all_system_db_tables
```

Run the following script to create the required stored procedures for the Intrusion Detector and the Vulnerability Analyzer in the system_db database:

```
% $SYSTEMHOME/db/db_procs/create_all_system_stored_procedures
```

System Database Schema

The following tables describe the System database schema used by both the Intrusion Detection and Vulnerability Analysis tools. The highlighted rows within the tables indicate a unique primary key.

Table 7-1 - Nodes Table Description

NODES Table			Description
NODE	char(8)	not null	Common Language Node Identifier
CLLI	char(11)	not null	Common Language Location Identifier
LATITUDE	numeric(7,5)	null	Latitude of node (Ex. 38.12651)
LONGITUDE	numeric(8,5)	null	Longitude of node (Ex. -76.87332)
NODE_TYPE	int	not null	Type of node: 0 = Unknown 1 = STP_NODE 2 = SSP Access Tandem Switch 3 = Operator Services SSP Switch 4 = SP/SSP End Office 5 = SCP 6 = AIN SCP
NET_CODE	int	not null	Network code of SS7 point code TBD
NET_CRITICALITY	numeric(7,3)	null	Vulnerability analysis node criticality raw score
CRITICALITY_SCORE	numeric(5,3)	null	Vulnerability analysis node criticality normalized score
OCCUPANT_COUNT	int	null	Number of people working at node facility
REMOTE_ACCESS	tinyint	null	External log on access to node (REMOTE_PUBLIC, REMOTE_PRIVATE)
SECURITY_OBSERVATION	bit	not null	Facility access monitoring (Yes/No)

Table 7-2 - Node Types

NODE_TYPES Table	Description

APPENDIX B
SOFTWARE USER'S MANUAL

NODE_TYPE	tinyint	not null	Type of node: 0 = Unknown 1 = STP NODE 2 = SSP Access Tandem Switch 3 = Operator Services SSP Switch 4 = SP/SSP End Office 5 = SCP 6 = AIN SCP
NODE_STRING	varchar(30)	not null	Textual description of node type: Unknown STP_NODE SSP Access Tandem Switch Operator Services SSP Switch SP/SSP End Office SCP AIN SCP

Table 7-3 - Links Table Description

LINKS Table			Description
LINKSET_NAME	char(8)	not null	GTE nomenclature for SS7 link set (Ex. [illegible])
NEAR_PCODE	char(11)	not null	The near end node point code: SS7 point code of STP (Ex. 240-180-000)
FAR_PCODE	char(11)	not null	The far end node point code: SS7 point code of STP, SSP or SCP (Ex. [illegible])
NUM_LINKS	tinyint	null	Number of physical links per link set
LINKSET_TYPE	char(2)	not null	GTE nomenclature for linkset type derived from LINKSET_NAME: AG = A-link to gateway switch AI = A-link to independent carrier switch AL = A-link to other LEC AM = A-link to mobile carrier AP = A-link to SCP AQ = A-link to AIN SCP AS = A-link to SSP access tandem switch AT = A-link to operator services SSP switch AU = A-link to SSP end office BI = B-link to independent carrier STP BM = B-link to mobile carrier STP BN = B-link to GTE non-mated STP BR = B-link to RBOC STP DI = D-link to independent carrier STP DM = D-link to mobile carrier STP DN = D-link to GTE non-mated STP
MEDIA_TYPE	tinyint	null	Physical link media: 0 = FIBER_MEDIA 1 = MICROWAVE_MEDIA 2 = SATELLITE_MEDIA 3 = COAX_MEDIA
TRANSMISSION_PROVIDER	tinyint	null	Transmission facilities service provider for

APPENDIX B
SOFTWARE USER'S MANUAL

LINKS Table			Description
			linkset designated by SS7 network point code (Ex. GTE = 240)
PERCENT_UTILIZATION	numeric(6,3)	null	Percentage of link capacity utilized (based on 56kbps)
PERCENT_GEN_EXTERNAL	numeric(6,3)	null	Percentage of link capacity generated outside of GTE network
SECURITY_ENCRYPTION	bit	not null	Linkset encryption capability (Ex. FALSE = 0)
SECURITY_MONITORING	bit	not null	Linkset monitoring capability (Ex. FALSE = 0)
POINT_CODE_SCREENING	tinyint	null	Type of STP point code screening employed on the linkset: 0 = NO_PCODE_SCREENING 1 = NETWORK 2 = NETWORK_CLUSTER 3 = NETWORK_CLUSTER_MEMBER
LOGIC_SCREENING	tinyint	null	Type of STP logic screening employed on the linkset: 0 = NO_LOGIC_SCREENING 1 = MESSAGE_CLASS 2 = MESSAGE_TYPE
NET_VULNERABILITY	numeric(5,3)	null	Vulnerability analysis inherent link vulnerability score
VULNERABILITY_SCORE	numeric(5,3)	null	Vulnerability analysis link vulnerability score based on critical node analysis

Table 7-4 - Link Services Table Description

LINKS_SERVICE Table			Description
LINKSET_NAME			
SERVICE			

Table 7-5 - SCP Table Description

SCP Table			Description
SCP_POINT_CODE	char(11)	not null	SS7 point code of Service Control Point
NUM_OF_SVCS	int	null	The number of services accessed by the SCP
LINK_OCCU_SUM	real	null	Summation of the link occupancy for all links directly connected to SCP node

APPENDIX B
SOFTWARE USER'S MANUAL

Table 7-6 - SCP Services Table Description

SCP_SERVICE Table			Description
SCP_POINT_CODE	char(11)	no null	SS7 point code of a Service Control Point
SERVICE	tinyint	no null	[illegible]
SSP_COUNT_BY_SVC	int	null	The number of SSP nodes that receive service from SCP node (Roll-up)
ROOT_STP_POINT_CODE	char(11)	no null	[illegible]

Table 7-7 - STP Table Description

STP Table			Description
STP_POINT_CODE	char(11)	no null	SS7 point code of a Signaling Transfer Point
SSP_COUNT	int	null	Number of SSP nodes directly connected to STP node
POTS_LINK_OCCU_SUM	real	null	Summation of the link occupancy for all links connected to STP node except links connected to a SCP node

Table 7-8 - STP Services Table Description

STP_SERVICE Table			Description
STP_POINT_CODE	char(11)	no null	SS7 point code of a Signaling Transfer Point
PARENT_STP_POINT_CODE	char(11)	no null	[illegible]
SERVICE	tinyint	no null	[illegible]
NUM_HOPS_TO_SCP	tinyint	null	The number of hops from STP node to the SCP node that supplies a particular service
SSP_COUNT_BY_SVC	int	null	The number of SSP nodes that receive service through STP node. This count

APPENDIX B
SOFTWARE USER'S MANUAL

STP_SERVICE Table			Description
			includes directly connected SSP nodes and SSP nodes of children STP nodes. (Roll-up)
LINK_OCCU_SUM_BY_SVC	real	null	Summation of the link occupancy for all links directly connected to STP node for a particular service

Table 7-9 - SSP Table Description

SSP Table			Description
SSP_POINT_CODE	char(11)	not null	SS7 point code of Service Switching Point
CUSTOMER_IMPORTANCE	tinyint	null	Ranking between 1 and 10 indicating relative importance of an SSP node in the vulnerability analysis (user input parameter)
LINK_OCCU_SUM	real	null	Summation of the link occupancy for all links directly connected to SSP node

Table 7-10 - SSP Service Table Description

SSP_SERVICE Table			Description
SSP_POINT_CODE	char(11)	not null	SS7 point code of Service Switching Point
SERVICE	tinyint	not null	[illegible]

Table 7-11 - Network Codes Description

NETWORK_CODES Table			Description
CODE_STR	char(3)	not null	CODE represented as a string (Ex. "240")
CODE	tinyint	not null	Numerical code of SS7 point code (Ex. 240)
CO	varchar(40)	not null	Company assigned to the network code (Ex. 240 is GTE Service Corp/Telephone Ops)

Table 7-12 - Trunk Neighbor Description

TRUNK_NEIGHBOR Table			Description
SW1_POINT_CODE	char(11)	not null	SS7 SSP point code of near end switch of trunk route
SW2_POINT_CODE	char(11)	not null	SS7 SSP point code of far end switch of trunk route

Table 7-13 - Locations Table Description

LOCATIONS Table	Description

APPENDIX B
SOFTWARE USER'S MANUAL

LOCATIONS Table			Description
CLLI	char(11)	not null	Common Language Location Identifier of network node (Ex. MNSSVAXA03T)
LOC	varchar(32)	null	Actual city and state location associated with CLLI (Ex. MANASSAS, VA)

APPENDIX C
SOFTWARE DESIGN DOCUMENT

TABLE OF CONTENTS

APPENDIX C
SOFTWARE DESIGN DOCUMENT

TABLE OF CONTENTS

LIST OF FIGURES

APPENDIX C
SOFTWARE DESIGN DOCUMENT

LIST OF TABLES

APPENDIX C
SOFTWARE DESIGN DOCUMENT

1. Scope

1.1 System Overview

The System Network and Signal Infrastructure Vulnerability Analysis and Intrusion Detection System (hereafter referred to as the system) is a software application capable of providing real-time protection to the U.S. telecommunications Signaling System No. 7 (SS7) infrastructure.

The goal of the system is to perform the following:

a) Determine the vulnerability of the SS7 network based on its topology and identify the network elements most vulnerable to intrusion.
a) Detect intrusions to SS7 links being monitored.
a) Provide a User Interface for operator control and status display in support of the above processes.

The system uses a Sun Microsystems's SPARC-20 platform, running the Solaris 2.5 operating system.

1.1 Document Overview

This Design Description (SDD) describes the design for the system. The system CSCIs is being modeled with the Object Modeling Technique (OMT) Object-Oriented Analysis/ Design methodology, using the Rational Rose/C++ Computer-aided Software Engineering (CASE) tools. This system software includes the following Computer Software Configuration Items (CSCIs):

a) Intrusion Detector (including SS7 Monitoring, User Interface, Anomaly Detection process)
a) Vulnerability Analyzer (User Interface, Vulnerability Analysis processes)
a) Topology Database

1. References

The documents identified below provide background material and are incorporated herein by reference.

	DOCUMENT No.	TITLE
[1]	ISO 9001	International Organization of Standards 9001
[2]	ANSI T1.111-1996	Signaling System Number 7, Message Transfer Part (MTP), American National Standards Institute Inc., 1996
[3]	ANSI T1.112-1996	Signaling System Number 7, Signaling Connection Control Part (SCCP), American National Standards Institute Inc., 1996
[4]	ANSI T1.113-1995	Signaling System Number 7, Integrated Services Digital Network User Part (ISDN), American National Standards Institute Inc., 1995
[5]	ANSI T1.114-1996	Signaling System Number 7, Transaction Capacity Application Part (TCAP), American National Standards Institute Inc., 1996
[6]	ANSI T1.116-1990	Signaling System Number 7, Operations, Maintenance and Administration Part (OMAP), American National Standards Institute Inc., 1990

APPENDIX C
SOFTWARE DESIGN DOCUMENT

1. CSCI-wide Design Decisions

This section presents the CSCI-wide design decisions, that is, the decisions common to all the CSCI's behavioral design and those of its software subunits. The following functionality resides in the Common Infrastructure of the software architecture, accessible to all other CSCIs.

1.1 Interprocess Communication (IPC)

These section details the UNIX System V IPC methods used to implement interprocess communication, whereby two or more processes communicate with each other to perform tasks. These three mechanisms, listed below, are available for use in the design as needed.

a) Message Queues
a) Semaphores
a) Shared Memory

Message queues are a preferred method for IPC since they are easier to manage and are easily ported to other processing environments. Shared memory is used when higher performance is required, since the data is shared rather than copied between the different data regions as is done in the implementation of message queues. The following subsections give an overview of each of the three IPC options.

1.1.1 Message Queue

The message queue allows multiple processes on the same machine to exchange formatted data by sending and receiving messages among themselves. The messages stored in a message queue are persistent, even when there is no process referencing the queue. Messages are removed from a queue only when processes explicitly retrieve them.

Within the Common Infrastructure library, a MessageQueue class is provided to interface to the embedded message queues of the UNIX kernel. It is through this interface that two independent processes are able to pass messages between each other. A typical class hierarchy utilizing the MessageQueue class is shown in Figure 0-1. Here, we see classes of different processes, the SERVER class and the CLIENT class, and their relationships with the MessageQueue class using the OMT notation.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

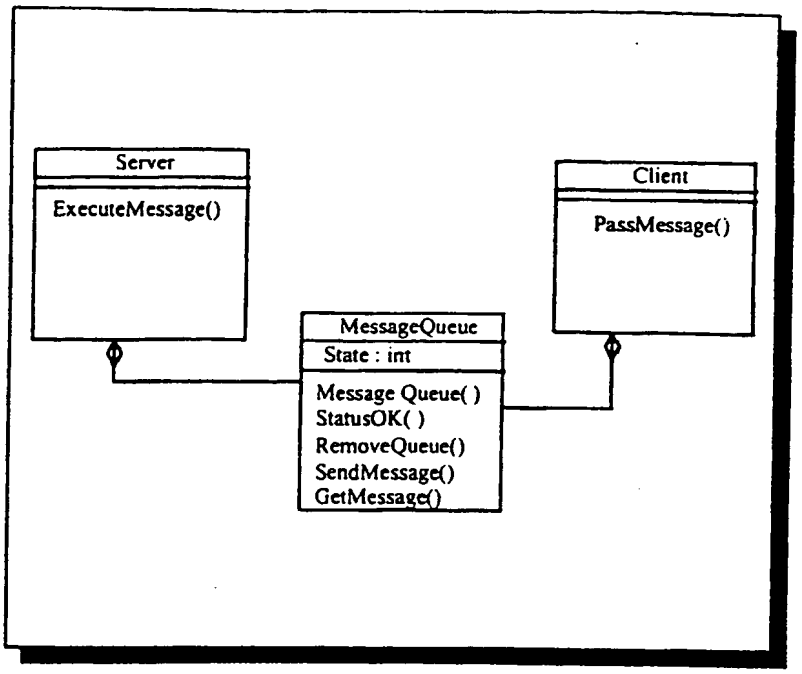


Figure 0-1 - Class Diagram: Message Queue

Figure 0-2 is an example scenario diagram showing how two independent processes can utilize the MessageQueue class. The SERVER and CLIENT objects must, first, instantiate their own MessageQueue objects using the MessageQueue constructor function. At this time, the IPC link is established. The status of the queue is then verified by the StatisOK() function. By using the SendMessage() and GetMessage() operations of MessageQueue class, the processes are able to pass messages between them.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

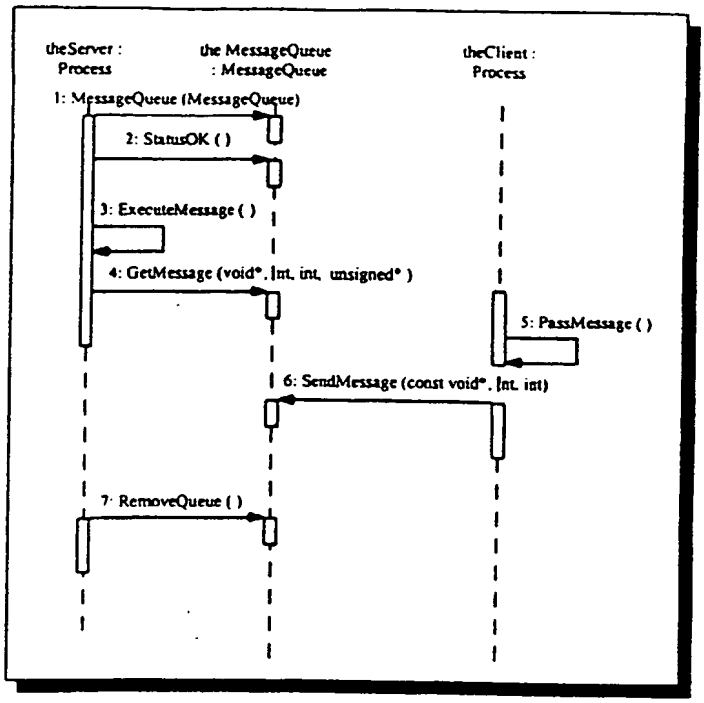


Figure 0-2 - Scenario Diagram: Passing a Message example

The following system-imposed limits on the manipulation of messages are defined in the <sys/msg.h> header file:

a) the maximum number of messages queues
a) the maximum number of bytes of data allowed for a message
a) the maximum number of bytes for all messages allowed in a queue
a) the maximum number of messages in all queues allowed in a system

1.1.1 Semaphore

Semaphores provide a method to synchronize the execution of multiple processes. Semaphores are frequently used along with shared memory to establish a method for IPC. Like messages, semaphores are persistent, despite their creator process's termination.

1.1.1 Shared Memory

Shared Memory allows multiple processes to map a portion of their virtual address space to a common memory region. Thus, any process can write data to a shared memory region and the data are readily available to be read and modified by other processes.

The data in a shared memory region are persistent. The memory space is not deallocated even if the process creating the shared memory region terminates. Also, shared memory does not provide any access control method for processes that use it, semaphores are used with the shared memory to implement this interprocess communication media.

1.1 Process Management

This section outlines the high-level generic process management scenarios of the System's Intrusion Detector. The following scenarios are addressed:

APPENDIX C
SOFTWARE DESIGN DOCUMENT

a) Initialization
a) Self-test operations

1.1.1 Initialization

Upon launching the System Intrusion Detector application, there are a set of generic software configuration and control scenarios that are performed. The following defines what is required and conforms to the set-up procedures of the system.

a) The Process Manager (within the Display Management) creates the following child processes:

i) the Intrusion Detection process
i) the Data Collection process

a) When the Process Manager (within the parent process) creates a child process, the Process Manager stores following information about the child:

i) the child's process identification assigned by the UNIX kernel
i) the system time at the time of creation
i) the file name EXECuting in the process
i) zero out statistics unique to the process

a) Once a child process is created, the child process initializes itself in the following matter:

i) prepares to send heart beat messages to the Process Manager.
i) close all unnecessary file descriptors
i) change working directory to ROOT. This allows unmounting of filesystem
i) reset the file access creation mask
i) run in background
i) disassociate from inherited process group by making the process group ID equal to process ID. Daemon no longer susceptible to signals sent to entire process group.
i) ignore terminal I/O signals
i) signals, process groups and control terminals revisited
i) disassociate from control terminal
i) don't reacquire a control terminal
i) handle SIGCLD signals

a) All processes open/create and initialize its message queue for IPC operations. Verify that the message queue status is operational.

a) Read relevant configuration information, if any, and configure based on that information.

a) At the completion of the process's initialization, each process waits for an indication (semaphore) from the parent process.

1.1.1 Self-Test

The section defines the implementation of the System's self-test requirements.

1.1.1.1 Process Verification

This section defines the requirements for process verification and management for the System applications. Each process will be monitored by the parent process using a heart beat IPC messaging.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

a) Once a child process is created, the child process prepares to send heart beat messages to the Process Manager at a fixed time interval of TBD seconds. The format of the heart beat message is as follows:

i) Message Type - indicating it is a heart beat message
i) Process Identification - assigned to the sending process during its creation.
i) Time of transmission - system time when the message was queued to the parent.
i) Process Stats - unique to the particular process.

a) Once the child process sends the heat beat message to the Process Manager (parent), the child process repeats the scenario in preparation for its next heart beat message when the next time interval is reached.

a) The Process Manager verifies that the child's operation is NORMAL using this heart beat message.

i) If the heart beat is received successfully, the Process Manager records the occurrence and stores the process's statistics for later reference.

i) If the heart beat is not received successfully, the Process Manager:

a) records this occurrence, via a counter
a) sends a KILL signal to the child
a) resets/restarts that process.
a) notifies the operator, via the GUI
a) records the event in a error log file.

1.1.1.1 Common Functional Verification

This section defines the implementation for software functional verification and management for the System applications. Each process will be monitored by the parent process using a heart beat IPC messaging.

a) Verify the status of the queues and check for OVERFLOW condition. The error is flagged and written to the local Operator Interface Status Queue.

a) Verify data for out-of-bounds condition.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

Architectural Design Overview

This section details the overall software architecture for the System. Figure 0-1 shows the data flow between the different processes and the external interfaces of the Intrusion Detector and the Vulnerability applications.
The architecture includes two (2) independent applications, the Intrusion Detector and the Vulnerability Analyzer, each with its own GUI environment. These processes and the interfaces are discussed in greater

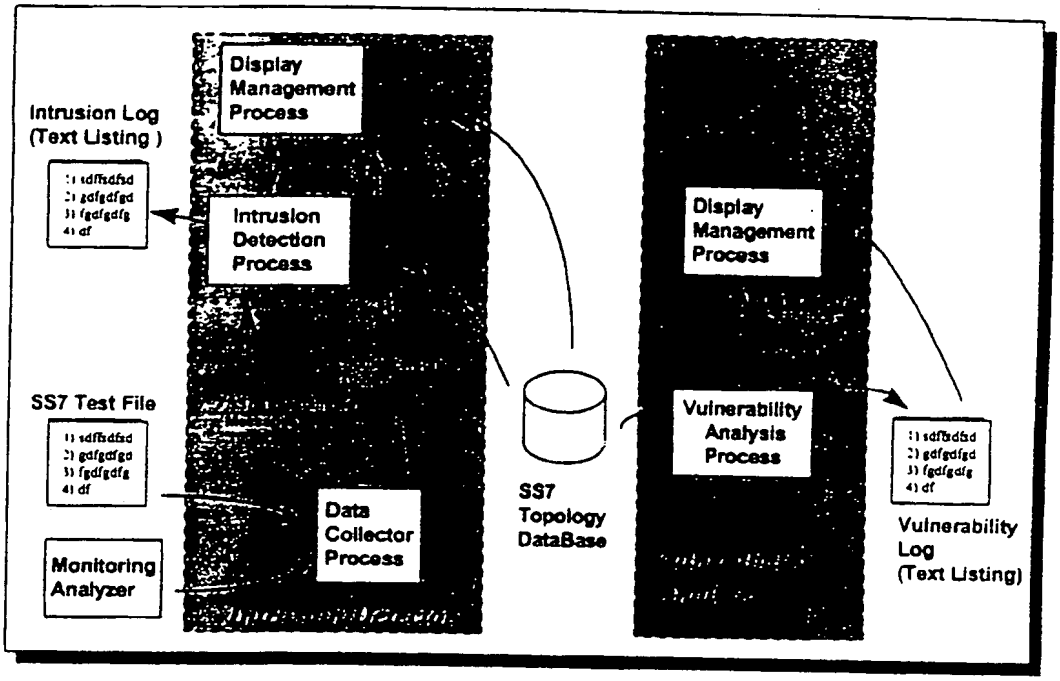


Figure 0-1 - Data Flow Diagrams

detail within the next subsections

a) The Intrusion Detector: A real-time application, including three concurrent processes: the Data Collection, the Intrusion Detection and it's Display Management processes.

a) The Vulnerability Analyzer includes two processes -- the Vulnerability Analysis and it's Display Management processes.

The system's class category diagram is shown in Figure 0-2 using the OMT notation. The class category diagram illustrates the logical collections of classes used by the applications. It maps well to the software architecture diagram presented earlier, however, the significance of this diagram shows the relationships and dependencies between these logical class groupings, including the Common Infrastructure category.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

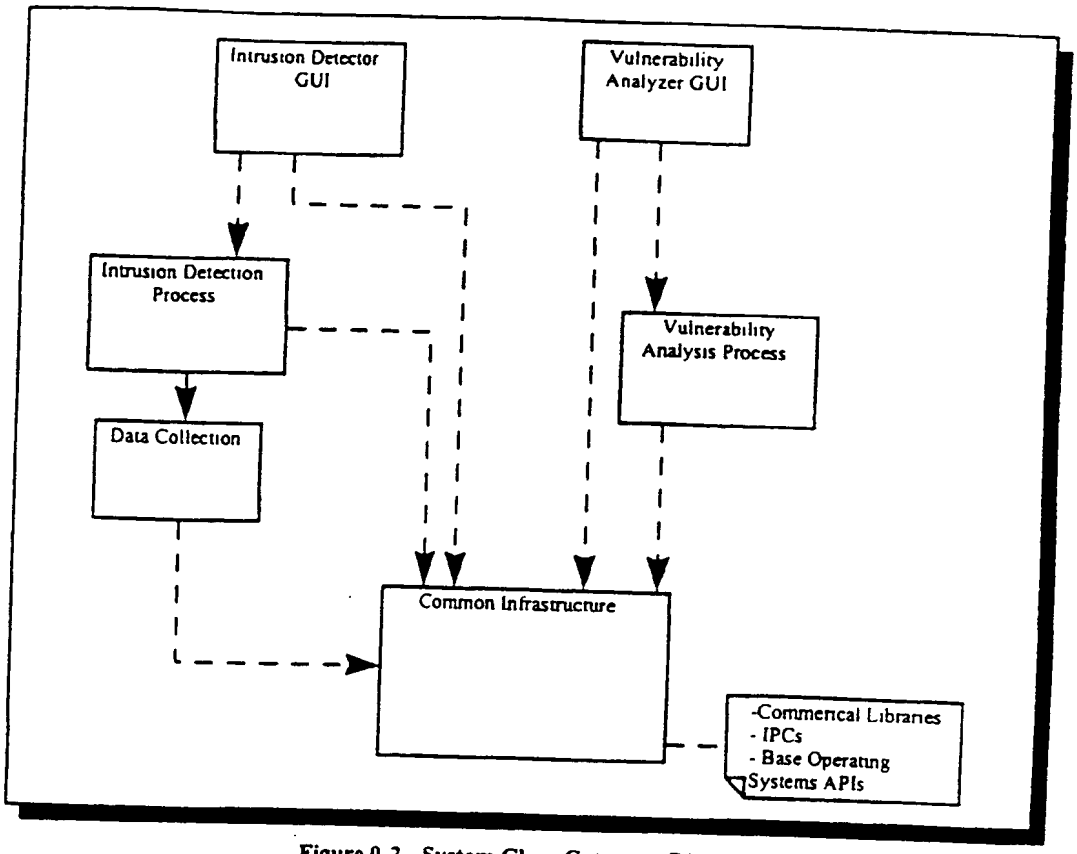


Figure 0-2 - System Class Category Diagram

The Common Infrastructure is an abstraction layer, used to isolate the rest of the application from the details of the low-level, operating system-specific functionality for portability to other platforms. It is a repository of common functionality of multiple processes (IPCs and database interfaces). It is implemented as a domain-specific framework or library, available to the higher-level subsystems to maximize reuse and standardization.

1.1 Intrusion Detector

This section describes the concept of execution and the IPC interfaces of the different processes that make up the System Intrusion Detector. The Intrusion Detector's architecture is partitioned into three (3) independent processes -- the Data Collection, the Intrusion Detection and it's Display Management processes.

1.1.1 Display Management Process

The Display Management process is the top-level or parent process of the Intrusion Detector and is available during system operation. This process includes the graphical user interface, designed using the SparcWork's Visual GUI builder and the Motif libraries, as well as operations for preparing the incoming data for user display. The look-and-feel of the environment is similar to that of the Open Windows environment.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

1.1.1.1 Interfaces

The following subsections identify the external interfaces of the Display Management process, as shown in the context diagram Figure 0-3. The message queue is the method used for all interprocess communication to and from the Display Management process.

1.1.1.1.1 Intrusion Detector Operator Console

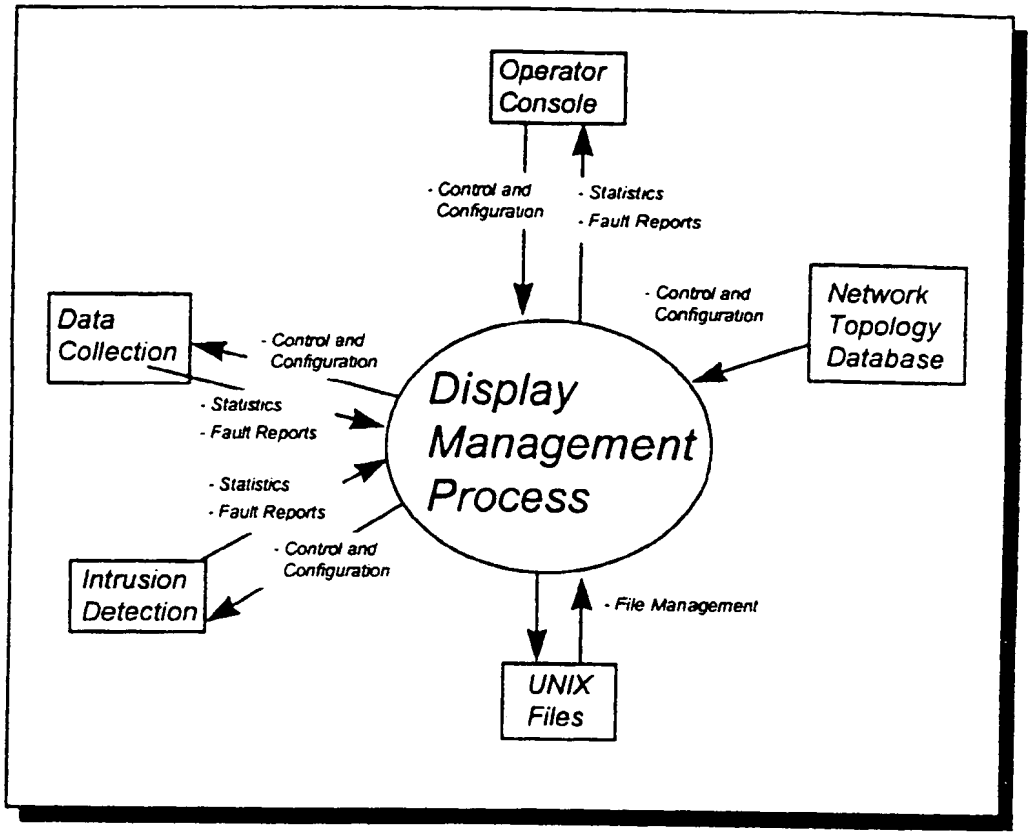


Figure 0-3 - Context Diagram: Intrusion Detector Display Manager

The operator console of the Intrusion Detector application is the GUI environment that allows the operator to change the application's operating parameters and observe predefined statistics, as well as overall system status.

1.1.1.1.1.1 Control and Configuration

In response to operator selection (via a pull-down menu), the following control and configuration options for the intrusion detection process are available. A dialog box is provided to the operator to enter the desired selection inputs.

a) File and Configuration Management: The control options for the system's configuration are listed below. When selected, another dialog box is displayed, prompting the operator for the desired filename:

APPENDIX C
SOFTWARE DESIGN DOCUMENT

i) Retrieve Configuration - retrieves a previously saved configuration file from the disk drive.
i) Save Configuration File - saves the current configuration settings to a file on the disk drive.
i) Retrieve Analysis File- retrieves a previously saved log file from the disk drive.
i) Save Analysis File - saves the most recent analysis results to a log file on the disk drive.
i) Exit - Aborts the application and all its associated processes.

a) View Management: The control options for the operator's viewing area are listed below. When selected, another dialog box is displayed, prompting the operator for the desired input(s):

i) Enter Monitoring Point(s): The operator indicates the current link(s) being monitored by the System. The node is entered using its point code designation and the links are identified by its linkset number. This action is acknowledged by a view of the local SS7 network topology displayed to the operator. **Bold** solid line(s), drawn to the corresponding far end node, indicates the links being monitored

a) Configuration Parameters: With these options the operator is able to adjust and define the threshold values used by this application. When selected, another dialog box is displayed, prompting the operator for the desired input(s).

a) Options: Miscellaneous options for test stimulus injection.

1.1.1.1.1.1 Statistics and Status Display

In response to an operator selection, the operator can view the following status/statistics. These statistics are maintained constantly by the Display Management process.

a) Network Topology Information: By clicking the mouse's right button on the desired node displayed on the topology view. This node information is provided to the operator in a scrollable text window. From that window, the operator can select a particular linkset of that node and view its characteristics.

a) Network Statistics: From the environment's main menu bar, the operator can request to view the capacity measurements listed below. Information is provided from the Intrusion Detection process at a fixed interval. A fault is logged if this message is not received in the expected time.

a) Anomaly Detection Indication: Information is provided from the Intrusion Detection process.

1.1.1.1.1 Intrusion Detection Process

This section details the Display Management process's interprocess communication to and from the Intrusion Detection process.

1.1.1.1.1.1 Control and Configuration

The following IPC messages are sent to the Intrusion Detection Process:

a) Operator Programmable Configuration Parameters:

i) MTP operation parameters.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

i) SCCP operation parameters.
i) ISUP operation parameters.

1.1.1.1.1.1 Statistics and Status Display

The following IPC messages are sent from the Intrusion Detection Process:

a) Anomaly Detection: In the event that any of the predefined anomaly rules or a combination of these rules are satisfied (indicating a detection), a message is sent to the Display Management process for display. The message will indicate the following information about the anomaly:

i) the SS7 message
i) a time stamp generated by the Data Collection process
i) the error code(s) assigned to the rule(s) fired which caused the anomaly report
i) the link affected
i) the Alarm type
a) NORMAL operation (initial display)
a) MINOR
a) MAJOR
a) CATASTROPHIC

a) Network Statistics: The following measurements are provided to the Display Management process at a fixed time interval. This message is also used by the Display Management process as a heartbeat indication from the Intrusion Detection process.

i) Total number of messages received per time tick
i) Number of MTP type messages received per time tick
i) Number of SCCP type messages received per time tick
i) Number of ISUP type messages received per time tick

1.1.1.1.1 Data Collection Process

This section details the Display Management process's interprocess communication to and from the Data Collection process.

1.1.1.1.1.1 Control and configuration

The following IPC messages are sent to the Data Collection Process:

a) Enable/disable test stimulus from file: When enabled, the Data Collection process will inject the test stimulus data into the real-time data stream.

a) Operator Programmable Configuration Parameters.

1.1.1.1.1.1 Status and Statistics

The following IPC messages are sent from the Data Collection Process. This message is also used by the Display Management process as a heartbeat indication from the Data Collection process.

a) Total number of messages per sec.
a) SS7 Link "Heart Beat" indication (as received from the Monitoring Analyzer)

1.1.1.1.1 Topology Database

The node and link information are retrieved by the Display Management process from the Topology database when the monitoring point is specified by the operator. This node and link information are detailed below:

APPENDIX C
SOFTWARE DESIGN DOCUMENT

a) Nodal Description
   i) Type (R_STP, STP, SSP, SCP, etc.)
   i) Point Code
   i) CLLI Code
   i) Office Name (city, state)
   i) Vendor Name (ATT, GTE, Sprint, etc.)
   i) Vulnerability Ranking of node (based on result of Vulnerability Analyzer)

a) Link Description
   i) Linkset Name (See Appendix 0)
   i) Type (A link, .., F link)
   i) Number of links in Linkset
   i) Occupancy (percentage usage)
   i) Media Type (copper, fiber, radio, etc.)
   i) Vulnerability Ranking of link (based on result of Vulnerability Analyzer)

1.1.1.1 Concept of Execution

The Display Management process implements the following functionality:

a) Operator Console Management
a) Process Management

1.1.1.1.1 Operator Console Management

Upon initialization, the Display Management process displays its operator console with all configuration parameters set to the factory default values (thresholds, etc.). It then waits for operator interaction. The operator will need to provide the configuration information listed below. This information can be loaded manually or via loading a pre-defined configuration flat file.

a) File Maintenance
a) Monitoring Point
a) Threshold values (if different from defaults)

1.1.1.1.1.1 Initialization

The Display Management process

a) Retrieve configuration file information

1.1.1.1.1.1 Initial Topology View Generation

Once entered, the monitoring point(s) are used to generate and display the local network topology view. The network topology view is based on topology information retrieved from the topology database (nodes, signal links, etc.). To implement, the GUI performs the following:

a) get the topology linkset for the first point-code entered from the operator.
a) if a monitoring point is an A-line, get its corresponding A-line mate to the end node and include in the drawing
a) if a monitor point is of a mated STP, draw the interconnecting lines of the STP mated pair.
a) draw local network - all direct links to the monitoring point are represented by a regular solid line. For clarity, the link(s) selected as being monitored, are represented by a bold solid line.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

1.1.1.1.1.1 Topology Maintenance

Once the local topology is drawn, the network view reflects the current state of each link of the local network to the operator using color coding. The link status is color coded, indicating the anomaly ranking (BLUE, YELLOW, ORANGE or RED): This anomaly ranking or state is based on the "Alarm type" data field from the anomaly detection message.

a) In response to an anomaly detection message from the Intrusion Detection process:

i) the corresponding link's anomaly status is updated and displayed in real-time on the topology view.

a) BLUE - normal operation (initial display)
a) YELLOW - caused by the reception of the "MINOR" alarm
a) ORANGE - caused by the reception of the "MAJOR" alarm
a) RED - caused by the reception of the "CATASTROPHIC" alarm

a) As the link's anomaly state is updated, the corresponding anomaly(ies) that caused the condition are buffered for operator display. The highest anomaly status of each link persists on the display until the operator acknowledges the corresponding alarms.

a) The operator acknowledgment clears the alarm buffer for that link and resets the link's anomaly state to "NORMAL operation" (BLUE).

1.1.1.1.1.1 Test Message Control

1.1.1 Data Collection Process

The Data Collector accepts pre-formatted SS7 message data from the SS7 monitoring source (via the communication port) and/or a UNIX file containing test messages. It is a real-time operation, whose primary function is to manage the communication port, as needed, and prepare the data for output to the next process in the real-time pipe -- the Intrusion Detection process.

1.1.1.1 Interfaces

The interfaces of Data Collector are shown in Figure 0-4. Each of these interfaces is detailed in the following subsections.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

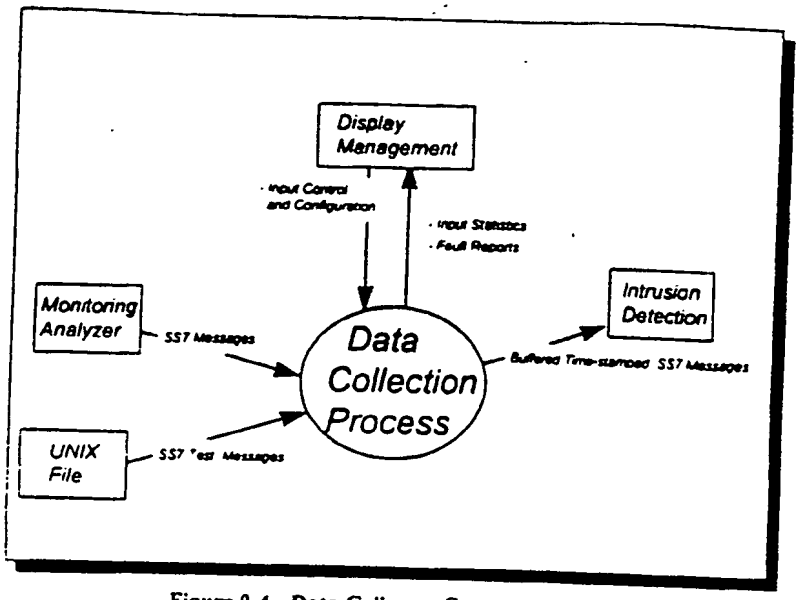


Figure 0-4 - Data Collector Context Diagram

1.1.1.1.1 **SS7 Input Message**

The incoming SS7 message, from the monitoring analyzer, is pre-formatted such that each message is of a fixed length with fixed information fields. The expected format for the SS7 message input is shown in Table 0-1.

Table 0-1 - Incoming SS7 Message Format

BYTES	
1	Network Indicator, Priority, Service Indicator
6	OPC / DPC
1	Message Type
5	Called Address (ISUP called digits)
5	Calling Address (ISUP called digits)
1	Called Party Subsystem Number
1	Global Title Translation Indicator (Boolean)
3	Called Party Point Code
1	Calling Party Subsystem Number
1	Global Title Translation Indicator (Boolean)
3	Calling Party Point Code
1	Data Type (UDT Messages)
1	Monitored link message originated
1	CIC (ISUP Message only)
1	CAUSE CODE (REL Message only)
3	Destination (MTP Transfer Message only)
1	Affected SSN (SCCP Management Message only)
3	Affected Point code (SCCP Management Message only)
1	Return Cause(SCCP Unidata Service Message only)
1	DCE or DTE indication

APPENDIX C
SOFTWARE DESIGN DOCUMENT

1.1.1.1.1 Intrusion Detection Process

The messaging to the Intrusion Detection Process includes the reformatted SS7 messages to be used in the intrusion determination. The output message format to the Intrusion Detection includes the following components:

a) the pre-formatted SS7 input message
a) a time stamp generated by the Data Collection process

1.1.1.1.1 UNIX Files

The Data Collection process will read and inject the test SS7 messages into the real-time message stream for purposes of testing. The format and the content of these test messages are identical to those from the monitoring analyzer.

1.1.1.1 Concept of Execution

With the continuing incoming SS7 messages from the communication port, it is a requirement that the data collection operate in real-time mode. Upon initialization of this process, the incoming SS7 messages are time stamped, reformatted and queued for the Intrusion detection process.

The top-level class diagram for the Data Collection process is shown is Figure 0-5. The following is a list of the classes, their responsibilities and the collaborations with the other classes.

a) The Data Collector class is the main class of this process. Its responsibility is to create and control its subclasses at a high level.
a) The MessageQueue class resides in the Common Infrastructure category. It is this class that represents the IPC method used by the Data Collector.
a) The CommPort class's responsibility is the control communication port and manages the data flow from the port. The SS7 message data structures are made available to the Data Collector class, independent of protocol used by the port.
a) The File class is the Data Collector's interface to the Unix files. The data structures of the test SS7 messages are made available to the Data Collector class, identical to that of the CommPort class.
a) The Clock class is used by the Data Collector as the main timer of the process.

A :NDIX C
SOFTWARE DESIGN DOCUMENT

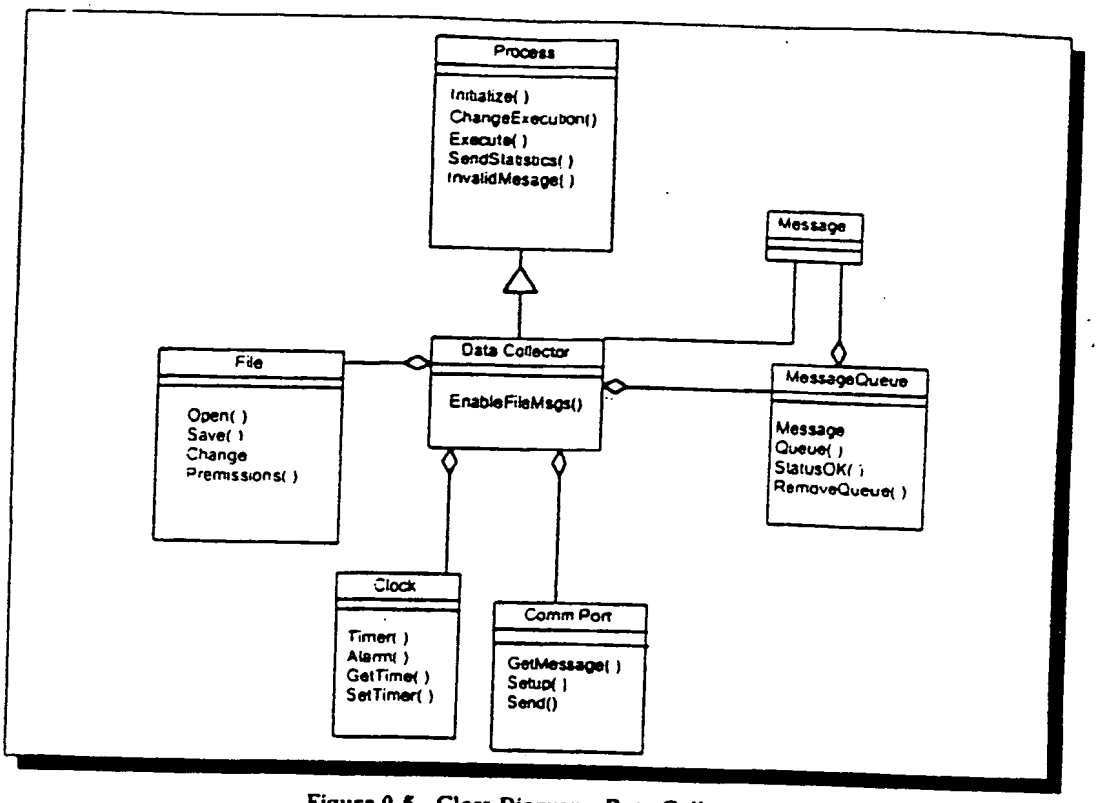


Figure 0-5 - Class Diagram: Data Collector

Figure 0-6 is the high level scenario diagram for initializing the of the Data Collection process. The function theDataCollector::Initialize() is called first and performs the required initialization implementation for the DataCollector class, as well as its subclasses. The following list details the function calls for Data Collector initialization:

a) theCommPort::CommPort() – this is the constructor of the CommPort class, which sets up the communication port for the specified protocol it is to implement.

a) theIntrusionQueue:: MessageQueue() – this is the constructor of the Intrusion Detection's MessageQueue class, which sets up the IPC link between the two processes.

a) theFile::FileDetected() – The DataCollector object verifies the existence of the test message file for injection. theDataCollector::EnableFileMsgs() is then called to set the proper local flags to enable this operation.

a) theClock::SetTimer() – The timer is setup and used to control the test message injection into the SS7 message stream from the UNIX file.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

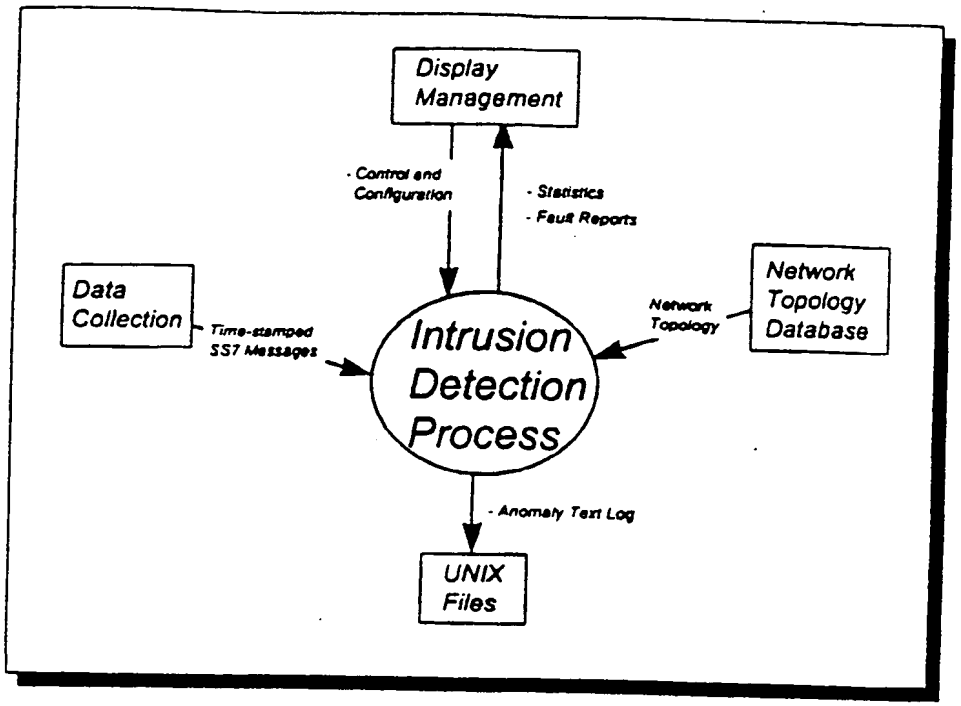


Figure 0-7 - Context Diagram: Intrusion Detector

1.1.1.1.1 Network Topology Database

The Network Topology Database provides the intrusion detection algorithms with the required relevant infrastructure data (node and link information) of the SS7 network. The network topology information and its format, as required for the intrusion detection, is identical to that used by the Display Management process.

1.1.1.1.1 UNIX Files

The Intrusion Detection process logs all anomalies detections, as well as the resultant intrusion decision. The filename is specified by the operator via the Display Management process.

1.1.1.1 Concept of Execution

The Intrusion Detection process reacts to an IPC message into its message queue. The thread of execution performed is based primarily on the type of this message. Any message type determined to be invalid are logged and discarded. The following messages are valid by this process:

a) Statistics Enable/Disable:
a) Fault Log Enable/Disable:
a) Process Start/Stop:
a) Process Shutdown:
a) Monitor Points:
a) SS7 MSU Record:

1.1.1.1.1 SS7 MSU Record

SS7 message is passed into its message queue from the Data Collection process. With every new message received, a determination is made whether any anomalies have indeed occurred.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

Along with the information contained within the newly received SS7 message itself, the detector uses the information from previously captured SS7 messages, as well as network topology information. It then correlates it results to predefined conditions or rules that would indicate the presence of an anomaly(ies). The following conditions are tested at different levels of the protocol.

a) ISDN User Part (ISUP) messages
   i) Improper RELEASE
   i) Improper BLOCKING and/or CIRCUIT GROUP BLOCKING
   i) Improper RESET and/or CIRCUIT GROUP RESET

a) Message Transfer Part (MTP) messages
   i) Improper CHANGEOVER (including Emergency Changeover)
   i) All improper TRANSFER PROHIBIT/RESTRICTED/CONTROLLED
   i) Improper LINK INHIBIT

a) Signaling Connection Control Part (SCCP) messages
   i) Improper Subsystem Prohibited
   i) Improper Subsystem Out of Service

Whether there was an anomaly detected or not, the current SS7 message is stored and used in future anomaly tests. The Intrusion Detection process logs all anomalies detections, as well as the resultant intrusion decision.

1.1 Vulnerability Analyzer

This section describes the concept of execution and the IPC interfaces of the different processes that make up the System Vulnerability Analyzer. The Vulnerability Analyzer's architecture is partitioned into two (2) independent processes, the Vulnerability Analysis and Display Management processes. The primary responsibility of the Vulnerability Analyzer is to evaluate an SS7 network topology and determine the locations most vulnerable to SS7 network intrusion.

1.1.1 Display Management Process

The Display Management process is the top-level or parent process of the Vulnerability Analyzer and is available during system operation. This process includes a window-based environment, similar to that used in the Intrusion Detector. This was purposefully done for two reasons:

1. It is hoped that similar environments (look-and-feel and positioning the control options under similar pull-downs) may make the tools more user-friendly
2. Maximize standardization and reuse of the design.

1.1.1.1 Interfaces

The following subsections identify the external interfaces of the Vulnerability Analyzer's Display Management process, as shown in the context diagram Figure 0-8. The Message queue is the method used for all interprocess communication to and from the Display Management process.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

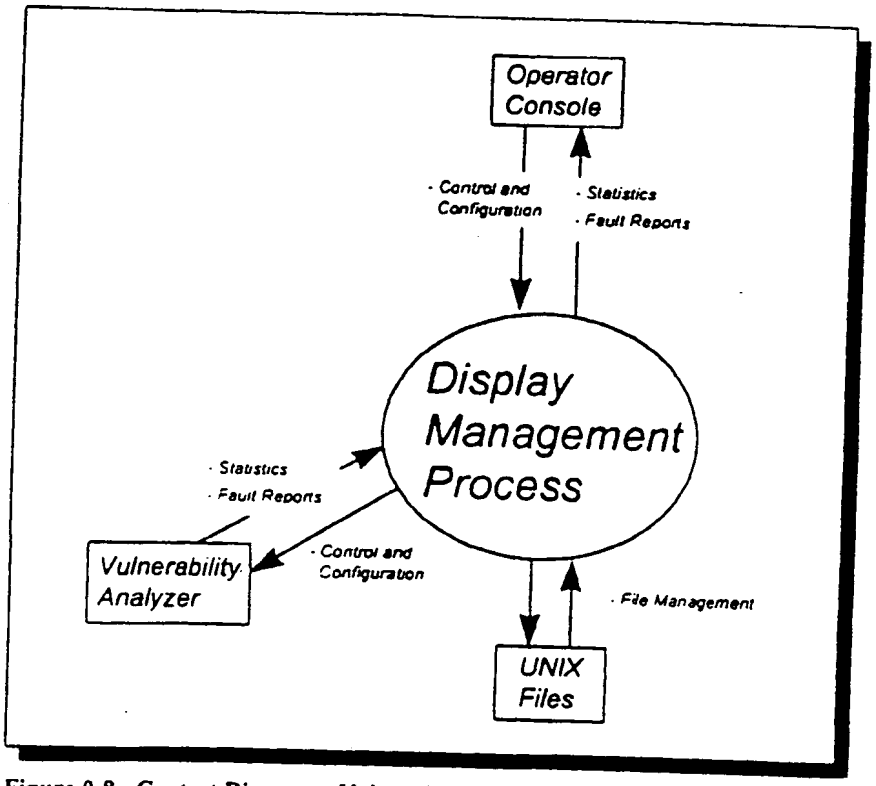


Figure 0-8 - Context Diagram: Vulnerability Analysis Process Display Manager

1.1.1.1.1 Vulnerability Analyzer Operator Console

The operator console of the Vulnerability Analyzer application is the GUI environment that allows the operator to change the application's operating parameters and observe predefined statistics, as well as overall system status.

1.1.1.1.1.1 Control and Configuration

In response to operator selection (via a pull-down menu), the following control and configuration options for the Vulnerability Analysis process are available. A dialog box is provided to the operator to enter the desired selection inputs.

a) File and Configuration Management: The control options of this pull-down menu is identical to that of the Intrusion Detector.

a) Thresholds: With these options the operator is able to adjust and defined the threshold values used by this application. When selected, another dialog box is displayed, prompting the operator for the desired input(s).

a) Analyze: The GO indication from the operator, is the signal to begin a new analysis of the network.

1.1.1.1.1.1 Network Vulnerability Display

APPENDIX C
SOFTWARE DESIGN DOCUMENT

In response to the ANALYZE COMPLETE message from the Vulnerability Analysis Process (indicating the analysis is complete), the Display Management process will then retrieve the vulnerability log UNIX flat file for operator display. The data fields of the display include the following information:

a) the Link or Node name and office name
a) the criteria satisfied indicating vulnerability
a) its vulnerability ranking

1.1.1.1.1 Vulnerability Analysis Process

This section details the Display Management process's interprocess communication to and from the Vulnerability Analysis process.

1.1.1.1.1.1 Control and Configuration

The following IPC messages are sent to the Vulnerability Analysis Process:

a) Operator Programmable Thresholds: These threshold parameters are used by the Vulnerability Analysis process in support of its algorithms.

a) Operational Control Messaging: The following indications are sent to the Vulnerability Analysis Process to control its flow of operation:

i) ANALYZE message – This indicates to begin its analysis using its current threshold set.

1.1.1.1.1.1 Status and Statistics

The following IPC messages are sent from the Vulnerability Analysis Process its Display Management process:

a) Operational Control Messaging: The following indications are sent from the Vulnerability Analysis Process, reflecting its operation status:

i) COMPLETE message – This indicates that its analysis has been completed and the log file is ready for operator display.

1.1.1.1 Concept of Execution

In response to an ANALYZE indication from the operator, the Vulnerability Analyzer's Display Management process sends its own ANALYZE indication to the Vulnerability Analysis Process.

Upon reception of the COMPLETE message from the Vulnerability Analysis Process, the Display Management process retrieves the specified Unix flat file containing the vulnerability log information, just calculated. It is then displayed to the operator via its own scrollable text display window.

1.1.1 Vulnerability Analysis Process

The Vulnerability Analysis evaluates the current SS7 network topology and ranks the each entity of the network infrastructure, based on its vulnerability to potential intrusions.

1.1.1.1 Interfaces

The context diagram, shown in Figure 0-9, identifies the multiple IPCs needed by this subsystem. The following subsections address these interfaces.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

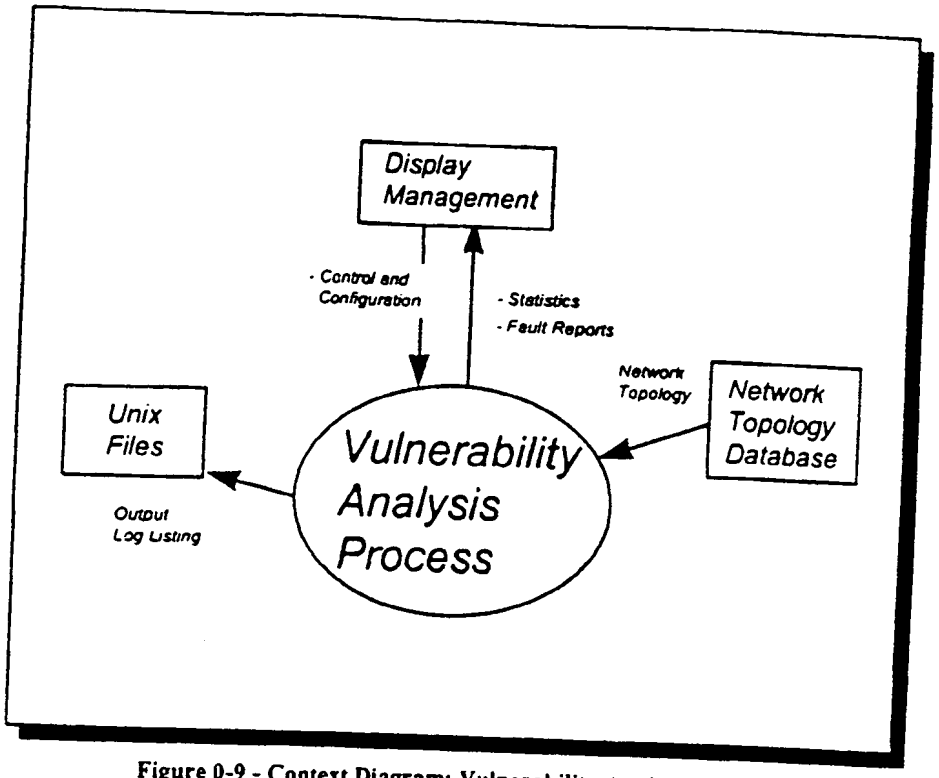


Figure 0-9 - Context Diagram: Vulnerability Analysis Process

1.1.1.1.1 UNIX Files

Once the analysis of the network is complete, the Vulnerability Analysis process records its results into a UNIX flat file for future retrieval and display by the Display Management process. The text fields in this text file are as follows:

a) the Link or Node name and office name
a) the criteria satisfied indicating vulnerability
a) its vulnerability ranking

1.1.1.1.1 Network Topology Database

The Network Topology Database provides the vulnerability analysis algorithms with the required relevant infrastructure data of the SS7 network . The network topology information and its format, as required for the vulnerability analysis, are listed below:

a) Numerical weights for Physical Accessibility of the each link and node.
a) Numerical weights for Functional Accessibility of the each link and node.
a) Numerical weights for Security Capability of the each link and node.
a) Numerical weights for Node Criticality of the each node, relative to the surrounding network.
a) Link and node information.

1.1.1.1 Concept of Execution

In response to an ANALYZE indication from the Display Management Process, this process analyzes and ranks each link and node within the GTE SS7 network on its potential vulnerability to intrusion.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

Information about the network's infrastructure is retrieved from its database (topology and link/node vulnerability relationships) and used in its algorithms. The following aspects of the network are analyzed for each vulnerability determination:

a) Physical characteristics - the media type used (copper, fiber, etc.)
a) Functional characteristics - the services provided on the link/node
a) Security characteristics - the existing screening measures (on-line, encryption, observation, etc.)
a) Node Criticality - the importance of the network element with respect to the its usage and capacity.
a) Redundancy - availability of alternate routing around element.

As a network entry is evaluated, a resultant message is sent to the specified text log file (UNIX flat file). This is the file that the Display Management Process retrieves for operator display.

At the completion of the analysis, a COMPLETION message is sent to the Display Management process, indicating that the analysis results are available for display.

1.1 Network Topology Database

The Network Topology Database is the persistent storage for the GTE SS7 network infrastructure. It contains all the nodal and link information required to implement both the Intrusion Detector and the Vulnerability Analyzer processes.

1.1.1 Interfaces

The context diagram, shown in Figure 0-10, identifies the multiple IPCs needed by this subsystem.

Access to the topology database, via the SYBASE SQL Server, is accomplished using the SYBASE "Open

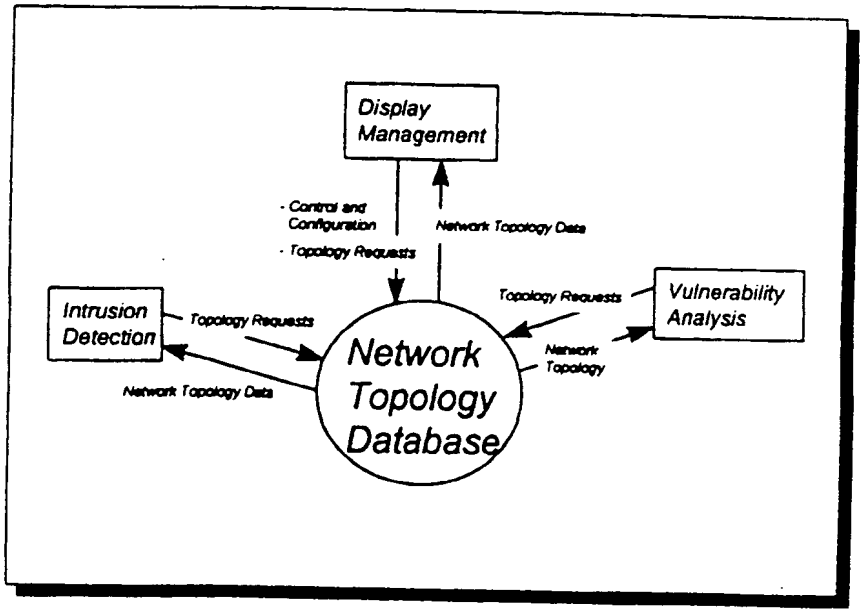


Figure 0-10 - Network Topology Database Domain Diagram

APPENDIX C
SOFTWARE DESIGN DOCUMENT

Client" Library. This three party library is a collection of utility routines that is our main interface to this database.

1.1.1 Concept of Execution

From the C++ environment, the Topology database is accessed via the DatabaseInterface class, whose external interface satisfies the operational requirements of the other processes. The DatabaseInterface class is a wrapper class, isolating the Open Client library function calls within itself and from the rest of the design.

In response to a function call, by a client process, to the DatabaseInterface class, the database returns the required data set as defined by its external interface functional signature.

Intrusion Detection Algorithms

This section presents a high-level detail of the specific algorithms used in determining the possibility of an anomaly event within the GTE SS7 network.

MTP Message Validation

All SS7 MSU messages of type MTP are analyzed for inconsistencies within their data fields as compared to the SS7 ANSI specification. The MTP tests described within this section are only performed on links currently being monitored by the Secure7 IDS.

a) The following SS7 MSU of type MTP are supported by the System Intrusion Detector:

   i) Changeover (CHANGEOVER, CHANGEOVER ACKNOWLEDGE, CHANGEBACK, CHANGEBACK ACKNOWLEDGE, EMERGENCY CHANGEOVER, EMERGENCY CHANGEOVER ACKNOWLEDGE)
   i) Transfer Prohibit/Restrict
   i) Signaling Route Set Test
   i) Transfer Allowed
   i) Transfer Control
   i) Signaling Route Set Congestion Test
   i) Management Inhibit (Link Inhibit, Link Inhibit Acknowledge, Link Local Test Signal, Link Remote Test Signal, Link Force Uninhibit, Link Uninhibit)

a) For all SS7 MSU messages, the following actions and checks will be performed.

   i) Maintain and threshold the number of occurrences of each of the MSU types and functions, on each SLC, to their corresponding adjustable threshold. An alarm is declared to the GUI and log file if the number of occurrences exceed its corresponding threshold.

   i) Validate SS7 routing label of each MSU. The link connection, based on the message's OPC and DPC, is verified against the information of the GTE Network topology database (LINK NEAREST NEIGHBOR test). An alarm is declared to the GUI and log file if a link relationship does not exist. This check will also verify originating point code (OPC) does not equal the designation point code (DPC).

MTP Messages

Upon reception, the following tests will be performed on all MTP messages.

a) **Changeover** - Upon reception of a CHANGEOVER MTP message, no additional tests are performed.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

a) **Emergency Changeover** - Upon reception of an EMERGENCY CHANGEOVER MTP message, no additional tests are performed.

a) **Changeover/Emergency Changeover Acknowledge** - Upon reception of a CHANGEOVER ACKNOWLEDGE MTP message, the following tests are performed.

i) Verify that a corresponding CHANGEOVER or EMERGENCY CHANGEOVER was previously detected on the same link. An alarm is declared to the GUI and log file if no previous Changeover was not detected.

a) **Transfer Prohibit/Restrict** - Upon reception of a TRANSFER PROHIBIT or a TRANSFER RESTRICT MTP message, the following tests are performed. The tests related to the destination point code, referred to by this message, is only done if that link is also being monitored.

i) Relative to the thresholding the number of occurrences of nodal and node cluster prohibits and restricts are maintained separately and thresholded to its corresponding adjustable threshold. An alarm is declared to the GUI and log file if the number of occurrences exceed its corresponding threshold.

i) Verify the OPC of this message, corresponds to a Signaling Transfer Point (STP). These message types are only expected to originate from a STP.

i) Verify the destination point code, referred to by this message, corresponds to a node directly connected to the originating STP in which the message was sent.

i) Verify that at least one of the following message types was previously detected on the destination link, referred to by this message. An alarm is declared to the GUI and log file if none of the following messages are detected (If the destination link, referred to by this message, is not part of the local topology defined, then this item will not be checked).

(1) EMERGENCY CHANGEOVER/CHANGEOVER - its DPC should be the same as the OPC of the original TRANSFER PROHIBIT/RESTRICT message on the other link

(1) LINK INHIBIT - its direction is irrelevant

(1) TRANSFER PROHIBIT - due to a STP broadcasting a link redirection.

a) **Signaling Route Set Test** - Upon reception of a SIGNALING ROUTE SET TEST MTP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that a TRANSFER PROHIBIT or TRANSFER RESTRICT message was previously detected on the same link in the opposite direction (OPCs and DPCs are reversed)

a) **Transfer Allowed** - Upon reception of a TRANSFER ALLOWED MTP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that a SIGNALING ROUTE SET message was previously detected on the same link in the opposite direction (OPCs and DPCs are reversed).

i) Verify that the total number of SIGNALING ROUTE SET TEST messages detected on this link, before a TRANSFER ALLOWED message, is greater than one (1) (SOFT ALARM).

APPENDIX C
SOFTWARE DESIGN DOCUMENT

i) Check for INVALID SLC INHIBIT patterns - This test analyzes the SLC inhibit patterns of each linkset and identifies any non-random inhibiting of consecutive SLCs of a linkset An adjustable number of consecutive SLCs inhibited are identified as an INTRUSION

a) **Link Local Test Signal** - Upon reception of a Management Inhibit a LINK LOCAL TEST SIGNAL MTP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that a LINK INHIBIT ACKNOWLEDGE message was previously detected on the same link in the opposite direction (OPCs and DPCs are reversed). This message must follow a LINK INHIBIT ACKNOWLEDGE message within the T20 timer period plus a processing delta time.

i) Verify that at least two (2) consecutive LINK LOCAL TEST SIGNAL messages are detected on the same link. The second message must follow the first LINK LOCAL TEST SIGNAL message within the T20 timer period plus a processing delta time.

a) **Link Remote Test Signal** - Upon reception of a Management Inhibit a LINK REMOTE TEST SIGNAL MTP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that a LINK INHIBIT ACKNOWLEDGE message was previously detected on the same link in the same direction (OPCs and DPCs are the same).

i) A LINK REMOTE TEST SIGNAL message must follow a LINK INHIBIT ACKNOWLEDGE message within the T21 timer period plus a processing delta time.

i) Verify that at least two (2) consecutive LINK REMOTE TEST SIGNAL messages are detected on the same link. The second message must follow the first LINK REMOTE TEST SIGNAL message within the T21 timer period plus a processing delta time.

a) **Link Force Uninhibit** - Upon reception of a Management Inhibit a LINK FORCE UNINHIBIT MTP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that a LINK LOCAL TEST SIGNAL message was previously detected on the same link in the opposite direction (OPCs and DPCs are reversed).

i) A LINK FORCE UNINHIBIT message must follow the LINK LOCAL TEST SIGNAL message within the T20 timer period plus a processing delta time.

a) **Link Uninhibit** - Upon reception of a Management Inhibit a LINK UNINHIBIT MTP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that a LINK REMOTE TEST SIGNAL message was previously detected on the same link in the opposite direction (OPCs and DPCs are reversed).

i) A LINK UNINHIBIT message must follow the LINK REMOTE TEST SIGNAL message within the T21 timer period plus a processing delta time.

APPENDIX C
SOFTWARE DESIGN DOCUMENT

ISUP Message Validation

All SS7 MSU messages of type ISUP are analyzed for inconsistencies within their data fields as compared to the SS7 ANSI specification. The ISUP tests described within this section are only performed on links currently being monitored by the Secure7 IDS.

a) The following SS7 MSU of type ISUP are supported by the Secure7 IDS:
   i) Initial Address
   ii) Address Complete
   iii) Release
   iv) Release Complete

b) For all SS7 MSU messages, the following actions and checks will be performed..

   i) Maintain and threshold the number of occurrences of each of the MSU types and functions to its corresponding adjustable threshold. An alarm is declared to the GUI and log file if the number of occurrences exceed its corresponding threshold.

   ii) Validate SS7 trunk connection between the message's OPC and DPC (TRUNK NEAREST NEIGHBOR test). An alarm is declared to the GUI and log file if a trunk relationship does not exist. This check will also verify originating point code (OPC) does not equal the designation point code (DPC).

ISUP Messages

Upon reception, the following tests will be performed on all ISUP messages.

a) **Initial Address** - Upon reception of a INITIAL ADDRESS ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE.

   i) Verify that the CIC, referenced by the INITIAL ADDRESS message, was not currently allocated.

a) **Address Complete**- Upon reception of a ADDRESS COMPLETE ISUP message, no additional tests.

a) **Release** - Upon reception of a RELEASE ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

   i) Verify that a INITIAL ADDRESS, ADDRESS COMPLETE or an ANSWER message was previously detected on the same link.

   i) Verify that the CAUSE CODE of the RELEASE message is code 16 (normal unspecified) or code 17 (busy condition).

   i) Maintain the number of occurrences of each of the following cause codes and threshold with their corresponding adjustable threshold. An alarm is declared to the GUI and log file if the number of occurrences exceed its corresponding threshold.

      Code 1: UNALLOCATED NUMBER
      Code 3: NO ROUTE
      Code 5: MIS-DAILLED TRUNK PREFIX
      Code 28: ADDRESS INCOMPLETE
      Code 79: SERVICE OR OPTION NOT IMPLEMENTED
      Code 81: INVALID CALL REFERENCE
      Code 95: UNSPECIFIED INVALID MESSAGE

APPENDIX C
SOFTWARE DESIGN DOCUMENT

Code 97: MESSAGE TYPE NON-EXISTENT
Code 99, 100: INVALID PARAMETER
Code 111: UNSPECIFIED PROTOCOL ERROR

ii) A response (a RELEASE COMPLETE message) must follow a RELEASE message within the predefined time period plus a processing delta time.

iii) Check for INVALID CIC RELEASE patterns - This test analyzes the CIC release patterns of each trunk and identifies any non-random releasing of consecutive CICs of a trunk. An adjustable number of consecutive CICs released are identified as an INTRUSION.

b) **Release Complete** - Upon reception of a RELEASE COMPLETE ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that a RELEASE or a RESET message was previously detected on the same link as the RELEASE COMPLETE message.

ii) Verify that a BLOCK message was previously detected on the same link, routed in the opposite direction (OPCs and DPCs are reversed) of the RELEASE COMPLETE message. The same direction indicates possible RESET inserted at far-end.

c) **Group Reset** - Upon reception of a GROUP RESET ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that at least two (2) consecutive GROUP RESET messages are detected on the same link in the same direction (OPCs and DPCs are the same).

ii) The second message must follow the first GROUP RESET message within a five (5) second time period plus a processing delta time.

d) **Reset** - Upon reception of a RESET ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that no RELEASE COMPLETE message was previously detected on the same link from the opposite direction (DPC and OPC are reversed) of the RESET message.

ii) Check for INVALID CIC RESET patterns - This test analyzes the CIC reset patterns of each trunk and identifies any non-random resetting of consecutive CICs of a trunk. An adjustable number of consecutive CICs released are identified as an INTRUSION.

iii) A response (a UNEQUIPPED message) must follow a RESET message within the predefined time period plus a processing delta time.

e) **Group Blocking** - Upon reception of a GROUP BLOCKING ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that at least two (2) consecutive GROUP BLOCKING messages are detected on the same link in the same direction (OPCs and DPCs are the same).

ii) The second message must follow the first GROUP BLOCKING message within a five (5) second time period plus a processing delta time.

f) **Block** - Upon reception of a BLOCK ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

APPENDIX C
SOFTWARE DESIGN DOCUMENT

i) Verify that no UNBLOCK ACKNOWLEDGE message was previously detected on the same link from the opposite direction (DPC and OPC are reversed) within fifteen (15) seconds of the BLOCK message.

ii) Check for INVALID CIC BLOCKING patterns - This test analyzes the CIC block patterns of each trunk and identifies any non-random blocking of consecutive CICs of a trunk. An adjustable number of consecutive CICs released are identified as an INTRUSION.

g) **Block Acknowledge** - Upon reception of a BLOCK ACKNOWLEDGE ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE.

i) Verify that a BLOCK or a GROUP BLOCK message was previously detected on the same link from the opposite direction (DPC and OPC are reversed).

ii) A response (a UNBLOCK message) must follow a BLOCK ACKNOWLEDGE message within a five (5) minute time period plus a processing delta time.

h) **Group Block Acknowledge** - Upon reception of a GROUP BLOCK ACKNOWLEDGE ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that a BLOCK or a GROUP BLOCK message was previously detected on the same link from the opposite direction (DPC and OPC are reversed).

ii) A response (a UNBLOCK message) must follow a GROUP BLOCK ACKNOWLEDGE message within a five (5) minute time period plus a processing delta time.

i) **Unblock** - Upon reception of a UNBLOCK ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that a corresponding BLOCK ACKNOWLEDGE or a GROUP BLOCK ACKNOWLEDGE message was previously detected on the same link from the opposite direction (DPC and OPC are reversed) with the following time restricts:

ii) No UNBLOCK message should not be received within fifteen (15) seconds of the BLOCK ACKNOWLEDGE message.

iii) The UNBLOCK message should be received within five (5) minutes of the BLOCK ACKNOWLEDGE message

j) **Unblock Acknowledge** - Upon reception of an UNBLOCK ACKNOWLEDGE ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that an UNBLOCK or GROUP UNBLOCK message was previously detected on the same link from the opposite direction (DPC and OPC are reversed).

k) **Unequipped Circuit** - Upon reception of an UNEQUIPPED CIRCUIT ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that a RELEASE, RESET, GROUP RESET, BLOCK or GROUP BLOCK message was previously detected on the same link from the opposite direction (DPC and OPC are reversed).

APPENDIX C
SOFTWARE DESIGN DOCUMENT

ii) Check for INVALID UNEQUIPPED CIRCUIT CIC patterns - This test analyzes the unequipped CIC patterns of each trunk and identifies any non-random blocking of consecutive CICs of a trunk. An adjustable number of consecutive CICs released are identified as an INTRUSION.

l) Circuit Query - Upon reception of a CIRCUIT QUERY ISUP message, the following tests are performed. An alarm is declared to the GUI and log file if any of the following conditions are FALSE:

i) Verify that no RELEASE COMPLETE message was previously detected on the same link from the opposite direction (DPC and OPC are reversed) of the CIRCUIT QUERY message. Also, that the CIRCUIT QUERY message is not within a five (5) second period of the RELEASE COMPLETE message.

Network Analysis
This section deals with a periodic analysis of the network as a result of the message flow and its effect of that network.

a) If a link is prohibited or restricted, as a result of a TRANSFER PROHIBIT or a TRANSFER RESTRICT MTP message, the following tests are performed, but only if the link to the destination point code, referred to by the a TRANSFER PROHIBIT or a TRANSFER RESTRICT MTP message, is being monitored.

i) verify that no traffic (of any protocol) is detected on the link to the destination point code, specified by the TRANSFER PROHIBIT or a TRANSFER RESTRICT MTP message.

ii) verify that no ISUP messages are detected to and from the node corresponding to the destination point code specified by the TRANSFER PROHIBIT or a TRANSFER RESTRICT MTP message.

b) Node Cluster unavailability activity is monitored. Maintain and threshold the number of occurrences of the following:

i) number of clusters down (network total).
ii) number of clusters down by destination.
iii) number of node down by destination. This is incremented with each node and cluster TRANSFER PROHIBIT or a TRANSFER RESTRICT MTP message.

c) Check for INHIBIT TIMEOUT VIOLATION

Linkset Identifier Naming Convention

This section outlines the NOC's linkset identifiers for each linkset in GTE's SS7 network. The 8-digit identifiers are assigned using the following convention:

1. 1st Character - Link Type

a) A - A links from SP/SSP/SCP to an STP pair
b) B - B links between non-mated STPs on the same level (peers)
c) C - C links between STPs in a mated pair
d) D - D links between non-mated STPs on different levels
e) local and regional pairs)
f) E - E links from SP/SSP to an additional STP

APPENDIX C
SOFTWARE DESIGN DOCUMENT

g) F - F links between STPs/SSPs (not connected to STPs)
h) X - Test links

2. 2nd Character - Link Destination

a) C - Mated STP
b) G - Gateway
c) I - Independent Company
d) L - Another LEC STP
e) M - Mobile/Cellular
f) N - Non-mated STP
g) P - SCP
h) Q - AIN SCP
i) R - RBOC STP
j) S - SSP Access Tandem Switch
k) T - Operator Services SSP switch
l) U - SP/SSP End Office
m) X - MGTS (test links)
n) Z - Protocol Converter

3. 3rd, 4th, 5th characters (identifies the GTE STP):

000	LNCLILXC01W	012	DRHMNCXM19W
001	BLTNILXD01W	013	DRHMNCXF19W
002	MRHDKYXA19W	014	FTWYINXA02W
003	LXTNKYXA11W	015	GRRTINXA01W
004	TAMPFLXA00W	016	MARNOHXC01W
005	CLWRFLXA001	017	DLWROHXA01W
008	OCQNVAXA19W	018	MRFDWIXA01W
009	MNSSVAXA19W	019	WAUSWIXA01W
010	ERIEPAXM01W	020	MSKGMIXK01W
011	EDNBPAXE01W	021	THRRMIXT01W
400	OFLNMOXA01W	510	BVTNORXB00W
401	WNVLMOXA01W	511	TGRDORXA00W
402	OFLNMOXA02W	512	PNHOHICO00W
403	WNVLMOXA02W	513	WPHUHICO00W
500	SNMNCAXP00W	514	DCSNTXXA01W
501	ONTRCAXP00W	515	BYTWTXXA01W
502	DNTNTXXA01W	516	LNBHCAXP00W
503	IRNGTXXA01W	517	ONTRCAXP01W
504	BOTHWAXB01W	518	SANGTXXA01W
505	EVRTWAXA00W	519	BWWDTXXA02W
506	PLSPCAXG00W	520	SNMNCAXP01W
507	INDICAXG00W	521	LNBHCAXP01W

APPENDIX C
SOFTWARE DESIGN DOCUMENT

508	SNBBCAXF00W	524	EVRTWAXA06W
509	SNTMCAXF01W	525	BOTHWAXB06W

APPENDIX D
VULNERABILITY ANALYSIS ATTRIBUTES AND ALGORITHMS

Overview

1. Link Vulnerability: Where is the most desirable link(s) from which to gain access to the Most Critical Node in the SS7 Network.
   a) Link Vulnerability is established based on inherent link attributes only such as:
      i) media type
      ii) provisioner: due to limitations, the provisioners by Linkset ID was assumed to be the same as the company owning the Far-end Node - this is generally NOT the case (GTE to GTE linksets likely use IXC carriers when traversing across LATA boundaries)
   b) Final rankings of the Link Vulnerability is suppose to de-rate the ranking based on the number of hops away from the Critical Node.

2. Node Criticality: What is the most important asset to the SS7 Network Operation based on the attack scenario.

3. The following User Inputs are used to influence the analysis:
   a) Designation of either POTS or AIN services as the mode of analysis
      i) due to the way STPs are "homed" (routed) based on the type of service being provided, certain attributes are effected by the selection
      ii) The node criticality calculations are directly effected:
         a) determines the SCP node criticality (or SCPs not considered when POTS only specified)
         b) the rollup of numbers of nodes gaining access via each STP for a particular service
   b) Designation of specific SSP(s) of particular importance:
      i) in order to evaluate impact to specific switches which may have VIP customers homed to them
      ii) effects the SSP node criticality only

4. The following assumptions and simplifications have been incorporated into the Vulnerability Analysis:
   a) all Test Linksets have been removed from the database (Linkset Ids = XX = MGTS Test links)
   b) C-linksets have been removed from the database Linkset Ids = CC)
      i) it is understood that all STPs have mated pairs for loadshare and fail-over.
      ii) # links with C-linksets may be a distinguishing factor among STP pairs
   c) the following SSP types were defaulted to SSP EOs - attributes /algorithms need development:
      i) Mobile SSPs (Linkset Ids = AM)
      ii) other LEC SSPs (Linkset Ids = AL)
      iii) Gateway SSPs (Linkset Ids = AG = International Gateway switches in HI)
   d) Site Personnel Occupancies unknown at this time all defaulted to midrange Vulnerability Ranking = 5

LINKS

Physical-media-type:

- ALL links will = FIBER

APPENDIX D
VULNERABILITY ANALYSIS ATTRIBUTES AND ALGORITHMS

Media Type	Functional Media
fiber	2
microwave	5
satellite	6
coax	9

Physical-media-provider:

Transmission Provider	Provider Vulnerability Ranking
GTE	1
AT&T	1
Sprint	2
MCI	4
Ameritech	5
Bell South	3
Southwestern Bell	4
Bell Atlantic	4
US West	6
Delta Communications	8
NTS Communications	8
PTI Communications	8
Norlite	8
Others	9

Functional-services: (attack desirability based on user scenario- USER INPUT).

Service Type	Location	rank
E800CA	SNMC/LNBH	
E800FW	FTWN/GRRT	
CRS	DNTN/IRVG	
INCONTACT	TMPA/CLWR	
LIDB_CNAM	FTWN/GRRT	

Functional-Capacity-%-Utilization

% Utilization	Functional Capacity
0- <5	1
5- <10	3
10- <15	5
15- <20	7
20- <25	8
>= 25	9

APPENDIX D
VULNERABILITY ANALYSIS ATTRIBUTES AND ALGORITHMS

Functional-capacity-% internally generated

% Internally Generated	rank
0-25	
25-50	
50-75	
75-100	

Functional-security-encryption:

- If the link is encrypted, then the overall Security Ranking = 1 (no other influences to Security)

type	Security
encrypted	1
not encrypted	null

Functional-security-screening:

- Currently screening ALL on EXTERNAL links.(far end Point Code NOT GTE (NOT= 240) use:

Point Code Screening	Logic Screening	Security Screening
Network and Cluster and Member	message class	5

- All others (far node Point code = GTE =240) use:

Point Code Screening	Logic Screening	Security Screening
NONE	ANY	9

Point Code Screening	Logic Screening	Security Screening
NONE	ANY	9
Network only	none	8
Network and Cluster	none	7
Network and Cluster and Member	none	6
Network only	message class	7
Network and Cluster	message class	6
Network and Cluster and Member	message class	5
Network only	message type	6
Network and Cluster	message type	4
Network and Cluster and Member	message type	3

Logical-number-LinksPerLinkset:

APPENDIX D
VULNERABILITY ANALYSIS ATTRIBUTES AND ALGORITHMS

- Note: if data becomes available on automatic alt routing and multiple Linksets then these attributes will need to be reconsidered. Currently, the multiplicity of routes will only be accounted for by the number of Links in each Linkset.

# of Links	rank
1	8
2	4
3	3
4	2
>= 8	1

Attribute Relationships (Algorithms)

Physical-media-type && Physical-Media-provider

Media Type	Physical Media-Access Rank
any	Media Type
Fiber	Fiber + (Provider Rank * 0.50)
microwave	microwave + (Provider Rank * 0.25)
coax	coax + (Provider Rank * 0.25)
satellite	

- Functional-Services-Multiple

Service	&& Service	&& Service	Ranking	Comment
ISUP				
OMAP	Calling Card	VPN	8 or 9	3 svc, 1 critical
E800				
E911	OMAP		10	2 critical
LNP				
Remote Call Fwd				
VPN	Calling Card		4 or 5	2 non-critical
Calling Card				

may use a formula such as:

- POTS only Functional Service = 5
- 1 service only = Service Ranking
- 2 non-critical (3 or 4) = most critical +1
- M && L = M
- M && M = M + 1
- M && H = H
- 1 non-critical && 1 critical = critical + 1 (max = 10)
- 2 critical (8 or 9) = 10
- 3 or more non-critical = most critical + 2

APPENDIX D
VULNERABILITY ANALYSIS ATTRIBUTES AND ALGORITHMS

LSTP-B-Links to non-GTE = POTS only

- Functional-Services && %Utilization by Service

Service	&& % Traffic used by Service	= Ranking
E911	< 10%	2 or 3
E911	>= 10%	8 or 9

  - E911 traffic >10% of total Utilization is considered high risk

- Functional Capacity && %-Utilization && Loadshare Links:
  - high &Utilization is far more serious on links with only 1 loadshare link; whereas, high %Utilization links with numerous loadshare links become have the vulnerability reduced (ideally in a 1/N relationship).
  - Since Functional Capacity Ranking is = %-Utilization Ranking at this point, then the multiplicity of Loadshare Links will only act to reduce the Functional Capacity Ranking...

% Utilization Rank	# of Links Rank	Functional Capacity	tota
1	1	Funct Capacity - 3	1
1	2	Funct Capacity - 2	1
1	4	Funct Capacity - 1	1
1	8	Funct Capacity	1
3	1	Funct Capacity - 3	1
3	2	Funct Capacity - 2	1
3	4	Funct Capacity - 1	2
3	8	Funct Capacity	3
5	1	Funct Capacity - 3	2
5	2	Funct Capacity - 2	3
5	4	Funct Capacity - 1	4
5	8	Funct Capacity	5
7	1	Funct Capacity - 3	4
7	2	Funct Capacity - 2	5
7	4	Funct Capacity - 1	6
7	8	Funct Capacity	7
8	1	Funct Capacity - 3	5
8	2	Funct Capacity - 2	6
8	4	Funct Capacity - 1	7
8	8	Funct Capacity	8
9	1	Funct Capacity - 3	6
9	2	Funct Capacity - 2	7
9	4	Funct Capacity - 1	8
9	8	Funct Capacity	9

- Physical-Connectivity-Internal && %Utilization && %GeneratedExternal:
  - Internal Connectivity = GTE for Transmission Provider
  - % Generated External = 0% for Far point code = GTE =240

(default of Tranmission Provider = Far Node Owner)

APPENDIX D
VULNERABILITY ANALYSIS ATTRIBUTES AND ALGORITHMS

% Generated External	= Functional Capacity
0	Funct Capacity
1 - 10	Funct Capacity + 0.5
11 - 20	Funct Capacity + 1
21 - 30	Funct Capacity + 1.5
31 - 40	Funct Capacity + 2
41 - 50	Funct Capacity + 2.5

- Physical-Connectivity-External && %Utilization && %Generated-External:

  - External Connectivity = NOT GTE for Transmission Provider
  - % Generated External = 50% for Far point code NOT= GTE NOT=240

  (default of Tranmission Provider = Far Node Owner)

% Generated External	= Functional Capacity
0	Funct Capacity
1 - 10	Funct Capacity + 1
11 - 20	Funct Capacity + 2
21 - 30	Funct Capacity + 3
31 - 40	Funct Capacity + 4
41 - 50	Funct Capacity + 5

- Functional-Capacity && Security-Monitoring:
  - Even though a link may be monitored, When a link is monitored, the Capacity ranking is decreased (less Vulnerability) but the degree to which the ranking is decreased still follows the logic that it is easier to hide intrusion messages in a higher occupancy link. The increase of traffic load and performance parameters on the link by inserted message traffic is again, less significant on a higher occupancy link. (where the occupancy is represented within the Capacity ranking - the higher Occupancy the higher the Capacity ranking)

  - Whether Monitoring exists or not is influencing the Capacity (% Utilization) ranking

Functional Capacity	&& Monitoring	= New Functional Capacity
any	false	Func Capacity
L	true	Func Capacity
M	true	Func Capacity - 2
H	true	Func Capacity - 1

- Functional-Security-Screening && Functional-Security-Monitoring:

Screening Rank	&& Monitoring	= Security
any	false	Screening
1,2,3,8,9,10	true	Screening - 1
4,5,6,7	true	Screening - 1

APPENDIX D
VULNERABILITY ANALYSIS ATTRIBUTES AND ALGORITHMS

- Functional-Services && Functional-Security:

Services Rank	&& Monitoring	= New Service Rank
any	false	Service Rank
1 or 2 or 3	true	Service Rank
4	true	Service Rank - (Security Rank * 0.75)
5	true	Service Rank - (Security Rank * 0.5)
6	true	Service Rank - (Security Rank * 0.25) -
7 or 8 or 9	true	Service Rank

- Service Ranking is influenced by Security only in the middle rankings

Link Level Relationships

- When physical access difficult then Vulnerability is not very influenced by other factors:
  - Physical Media Access <= 3 && Functional Services 8,9,10 && Functional Capacity 8,9,10 = Physical Media Access +1
  - Physical Media Access <= 3 && any other influences
    Link Vulnerability = Physical Media Access

- When physical access is mid-range Vulnerability is most heavily influenced by Security:
  - Physical Media Access >=4 , <=7
    && Functional Services 8,9,10
    && Functional Capacity 8,9,10
    && Security 1,2,3
    Link Vulnerability = Security + 1/2

- When physical access is mid-range and Security is also mid-rangeVulnerability is influenced by Functional Services and Functional Capacity equally:
  - Physical Media Access >=4 , <=7
    &&Security >=4 , <=7
    Link Vulnerability =

Functional Services	Functional Capacity	Vulnerability Total
H	H	Average of Scores
H	L	Average of Scores
L	H	Average of Scores
L	L	Average of Scores
M	M	Average of Scores + 1
M	H	Highest Score
M	L	Highest Score

APPENDIX D
VULNERABILITY ANALYSIS ATTRIBUTES AND ALGORITHMS

L	M	Highest Score
H	M	Highest Score

- When physical access is mid-range and Security is high-range Vulnerability is influenced by Functional Services and Functional Capacity equally but further degraded by poor Security:

  - Physical Media Access >=4 , <=7
  &&Security >=8 , <=10
  Link Vulnerability =

Security	Functional Services	Functional Capacity	Vulnerability Total
H	H	H	Average of Scores - 1
H	H	L	Average of Scores - 1
H	L	H	Average of Scores - 1
H	L	L	Average of Scores - 1
H	M	M	Average of Scores - 2
H	M	H	Highest Score
H	M	L	Highest Score
H	L	M	Highest Score
H	H	M	Highest Score

- When physical access is high-range Vulnerability is not influenced very heavily but is modified as follows:

Security	Functional Services	Functional Capacity	Vulnerability Total
H	H	H	Physical Access Score
H	H	L	Physical Access Score
H	L	H	Physical Access Score - 1
H	L	L	Physical Access Score - 2
H	M	M	Physical Access Score- 1
H	M	H	Physical Access Score
H	M	L	Physical Access Score - 1
H	L	M	Physical Access Score - 1
H	H	M	Physical Access Score
M	H	H	Physical Access Score
M	H	L	Physical Access Score - 1
M	L	H	Physical Access Score - 1
M	L	L	Physical Access Score - 3
M	M	M	Physical Access Score- 2
M	M	H	Physical Access Score- 1
M	M	L	Physical Access Score - 2
M	L	M	Physical Access Score - 3
M	H	M	Physical Access Score -1
L	H	H	Physical Access Score -1
L	H	L	Physical Access Score - 2
L	L	H	Physical Access Score - 3
L	L	L	Physical Access Score - 3

APPENDIX D
VULNERABILITY ANALYSIS ATTRIBUTES AND ALGORITHMS

L	M	M	Physical Access Score- 2
L	M	H	Physical Access Score- 1
L	M	L	Physical Access Score - 2
L	L	M	Physical Access Score - 3
L	H	M	Physical Access Score -2

Correlation of the Node Criticality Ranking into the overall Link Vulnerability:

- The inherent vulnerabilities of each link should be reconciled with the desirability of intruding upon the link to gain access to the most desirable node in the network. Ideally, it is more desirable to intrude onto a link directly connected to the most desirable node, Hence, the further away from the most desirable node the less desirable (less vulnerable) the link becomes.

Location-Number-transfers-to-critical-node: (Critical Node must first be determined)

Number of Hops	Ranking
0 (direct connect)	Vulnerability
1	Vulnerability - 1
2	Vulnerability - 3
3	Vulnerability - 6
4	Vulnerability - X
5	Vulnerability - Y

- this ranking uses the concept that the further from the intrusion occurs from the desired target, the less likely the attack has at success due to routing/ screening, etc.

Node Attributes

Default Node Rankings:

Node Type	Ranking
STP	7
SSP Tandem	6
SSP End Office	3
SSP TOPS	
SCP	

Node-criticality:

SCP Node Criticality =(Average of Service Desirability Rankings) * Σ (SSPs w/ access via SCP to desired service) * (Normalized Node Capacity)

- Σ (SSPs w/ access via SCP to desired service) = 100% since each service is implemented only in one place ** EXCEPT CNAME (CA and Ft Wayne) ** => need to have routing info in place for CNAME service - East / West division follows.

- when POTS is defined, the SCP Node Criticality is null

APPENDIX D
VULNERABILITY ANALYSIS ATTRIBUTES AND ALGORITHMS

- Average of Service Desirability = Σ(score of all services) / (num of services at SCP)

- Normalized Node Capacity = Σ(link occupancy for all links at node) / Σ(link occupancy for all links in region)

Node-criticality

STP Node Criticality:

- is influenced by the User Input of the Critical Service Rankings:
  - Critical Service Ranking is used to determine SCP locations providing access to the (N) highest ranked service(s) -
  - Determining Most critical SCP must account for combined ranking(s) of the (each) service accessed by the SCP (Average of Service Desirability Rankings at that SCP)
  - Critical SCP Location is then used to determine the Number of Hops to the Critical Service from each STP
  - Number of Hops to the Critical Service is used to determine the STP Node Criticality

- **STP Node Criticality =**
$\Sigma_{service=1}^{N}$ **(Service Ranking * Σ_{rollup} (SSPs $_{service}$) * Normalized Node Occupancy$_{service}$)**
/ (Σ_{all} (SSPs) * Number of Hops to Critical SCP)

- **POTS STP Node Criticality = Σ (SSPs w/ access via STP to desired service) * (Normalized Node Capacity)**

  - **Normalized Node Occupancy$_{service}$ = $\Sigma_{service}$(link occupancy for all links at node) / (Total Link Occupancy)$_{service}$**

  - Average of Service Desirability = Σ(score of all services) / (number of services via STP) / (number of STPs at same number of hops from critical service)
    - when POTS is defined, number of hops replaced by number of STPs at same level in network (if node is LSTP then divide by number of LSTPs connected to parent RSTP; if node is RSTP then divide by number of RSTPs)

    - determining the Number of Hops to Critical Service may be determined by starting at the location of the Critical SCP and working backward into the network traversing each chain of links back through each RSTP to each LSTP- as each STP is encountered, the count for the number of hops is to be noted for each STP.

  - for LSTPs: Σ SSPs are those SSPs directly connected to STP
  - for RSTPs Σ SSPs are all SSPs connected to the subtended LSTPs

Node-criticality (cont'd):

SSP Node Criticality = Default Node type Score * Customer Importance * Normalized Node Capacity

- Customer Importance = ranking input by user to indicate a high priority user homed to specific switch(es)

APPENDIX D
VULNERABILITY ANALYSIS ATTRIBUTES AND ALGORITHMS

- Normalized Node Capacity = Σ(link occupancy for all links at node) / Σ(link occupancy for all links in region)

Overall Node-Criticality :

Owner	Network Code	Node Owner Vulnerability Ranking	Ranking
Internal	240	1	Criticality + (0.5 * Ranking)
AT&T	215	1	Criticality + (0.5 * Ranking)
MCI	244	2	Criticality + (0.5 * Ranking)
Sprint	253	4	Criticality + (0.5 * Ranking)
Bell Atlantic	246	5	Criticality + (0.5 * Ranking)
Bell South	252	3	Criticality + (0.5 * Ranking)
Pacific Bell	251	4	Criticality + (0.5 * Ranking)
Ameritech	250	4	Criticality + (0.5 * Ranking)
US West	248	6	Criticality + (0.5 * Ranking)
LCI	001-016	8	Criticality + (0.5 * Ranking)
others		8	Criticality + (0.5 * Ranking)

Capacity-number-alternates: (how many other nodes can provide same function in auto alt routing- ignore SSPs)

Alt Nodes Avail	Ranking
1	Criticality - 2
> 1	Criticality - 5/6

- implies all other directly connected STPs at same level with routes toward same service

Security-physical:

Access	Ranking
occupied <10	Criticality - 1
occupied 10 -15	Criticality
occupied >15	Criticality + 1 (too many people to control)
Unoccupied	Criticality + 3

APPENDIX D
VULNERABILITY ANALYSIS ATTRIBUTES AND ALGORITHMS

	(max = 8)
remote private	Criticality
remote public	Criticality + 2

Security-observation:

Observation	Ranking
exists	Criticality - 5
not exist	Criticality

- Physical security alarming monitoring: access, door open, logon reporting.

APPENDIX E
INTRUSION DETECTION ALGORITHMS

MTP:

- **Changeover** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, SLC)
  - Threshold number of occurrences
  - LINK_NEAREST_NEIGHBOR (check OPC and DPC are on collected link)

- **Changeover Ack** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, SLC)
  - CORRELATE_TO_CHANGEOVER || CORRELATE_TO_EMER_CHANGEOVER (no previous Changeover indicates Changeover requested from another source)

- **Emergency Changeover Ack** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, SLC)
  - CORRELATE_TO_CHANGEOVER (no previous Changeover indicates Changeover requested from another source)

- **Emergency Changeover** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, SLC)
  - Threshold number of occurrences (very low)
  - LINK_NEAREST_NEIGHBOR (check OPC and DPC are on collected link)

- **Transfer Prohibit** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, DESTINATION)
  - Node and Cluster cases
  - LINK_NEAREST_NEIGHBOR (check OPC and DPC are on collected link) && OPC_STP (only sent from STPs)
  - CORRELATE_TO_DESTINATION (if DESTINATION point code is monitored)
    - check DESTINATION point code is 1 removed from OPC node
    - CORRELATE_TO_CHANGEOVER (check link to the DESTINATION point code for :
      - previous **Changeover**
      - || LSSU
      - || FISU)
    - CORRELATE_TO_LINK_INHIBIT (outgoing case: check link to the DESTINATION point code for receipt of **Link Inhibit** from an adjacent STP referencing a link toward particular node)
    - CORRELATE_TO_TRANSFER_PROHIBIT (outgoing case: check link to the DESTINATION point code for receipt of **Transfer Prohibit** from an adjacent STP)
    - case B or D-links CHECK_OPCs
      - **Scenario:** Once the STP sends a Transfer Prohibit or Transfer Restrict message additional message traffic from the DESTINATION node should not occur. Therefore, any messages to/from (especially from) the STP with the OPC = DESTINATION indicates that the Transfer message probably was not sent by the STP and may have been inserted on the link.

  {
  - if OPC or DPC of any message = DESTINATION then ALARM

  }

- **Transfer Restrict** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, DESTINATION)
  - Node and Cluster cases
  - LINK_NEAREST_NEIGHBOR (check OPC and DPC are on collected link) && OPC_STP (only sent from STPs)
  - CORRELATE_TO_DESTINATION (if monitored)
    - check DESTINATION point code is 1 removed from OPC node
    - CORRELATE_TO_CHANGEOVER (check link to the DESTINATION point code for :
      - previous **Changeover**
      - || LSSU
      - || FISU)

APPENDIX E
INTRUSION DETECTION ALGORITHMS

- CORRELATE_TO_LINK_INHIBIT (outgoing case: check link to the DESTINATION point code for receipt of **Link Inhibit** from an adjacent STP referencing a link toward the DESTINATION node)
- CORRELATE_TO_TRANSFER_PROHIBIT (outgoing case: check link to the DESTINATION point code for receipt of **Transfer Prohibit** from an adjacent STP)

- case B or D-links CHECK_OPCs
  - **Scenario:** Once the STP sends a Transfer Prohibit or Transfer Restrict message additional message traffic from the DESTINATION node should not occur. Therefore, any messages to/from (especially from) the STP with the OPC = DESTINATION indicates that the Transfer message probably was not sent by the STP and may have been inserted on the link.

{
- if OPC or DPC of any message = DESTINATION then ALARM

}

- **Signaling Route Set Test (T10 expires)** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, DESTINATION)
  - **Scenario:** When an STP sends a Transfer Prohibit or Transfer Restrict message the receiving node will initiate a Test Message transaction over the same link as the Transfer message. Therefore a Test Message should always be preceded by a Transfer message. Once the STP sends a Transfer Prohibit or Transfer Restrict message additional message traffic to or from the DESTINATION node being referred should not occur. Also, if a Transfer Allowed is the immediate response to the 1st Test Message then this may indicate that the Test Message may have been the result of an inserted Transfer Prohibited or Transfer Restricted message at the Test Message OPC node.
  - COUNT_CONSECUTIVE
    count the number of consecutive Test Messages which did not receive a Transfer Allowed response
  - CORRELATE_TO_TRANSFER
    {
    - case: Test for Prohibit
      {
    - CORRELATE_TO_TRANFER_PROHIBIT(if a previous Transfer was not SENT by STP re: Destination, indicates far-end got bogus Transfer)
      }
    - case: Test for Restrict
      {
    - CORRELATE_TO_TRANFER_RESTRICT (if a previous Transfer was not SENT by STP re: Destination, indicates far-end got bogus Transfer)
      }

    - if FAIL of BOTH correlations then ALARM
    }

- **Transfer Allowed** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, DESTINATION)
  - CORRELATE_TO_TRANSFER
    - **Scenario:** If a Transfer Prohibit or Restricted message in the same direction, did not precede a Transfer Allowed message this may indicate that a Transfer Prohibit or Restricted message was inserted at the Allowed OPC node on a different link

    {
    - if FAIL then ALARM
    }
  - CORRELATE_TO_1st_TEST_MESSAGE

APPENDIX E
INTRUSION DETECTION ALGORITHMS

- **Scenario:** If a Transfer Allowed is the immediate response to the 1st Test Message then this may indicate that the Test Message may have been the result of an inserted Transfer Prohibited or Transfer Restricted message at the Test Message OPC node

{

- if Test Message counter: = 1 then ALARM
- Threshold Number of occurrences of Transfer Allowed reply to 1st Test Message

}

- **Link Unihibit** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, SLC)
  - CORRELATE _TO_INHIBIT_ACK_T14
    {
    - if occurs before Ack or Denied or Timeout
      then =>ALARM (possible Uninhibit insertion or Response to inserted Link Inhibit)

    }
  - CORRELATE_TO_REMOTE_LINK_TEST
    {
    - if no Remote Link Test || if response to Local Link Test
    - => ALARM (possible Response to inserted Link Inhibit from different link or Uninhibit inserted)

    }
    - Threshold number of times Link Uninhibit is response to 1st Test cycle

- **Link Force Unihibit** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, SLC)
  - CORRELATE _TO_INHIBIT_ACK_T14 (no Uninhibit until Inhibit Ack or timeout)
  - CORRELATE _TO_LOCAL_LINK_TEST
    {
    - if no Local Link Test || if response to Remote Link Test
    - => ALARM (possible Response to inserted Link Inhibit from different link or Uninhibit inserted)

    }
  - Threshold number of times Link Force Uninhibit is response to 1st Test cycle

- **Link Inhibit** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, SLC
  - Threshold number of occurrences within Timeperiod
  - CHECK_FOR_PATTERNS_SLC
  - LINK_NEAREST_NEIGHBOR (check OPC and DPC are on collected link)

    - case: LOCAL_INHIBIT (Link_Inhibit sent from node)
      {
      - while T14 not expired && (Inhibit Ack or Inhibit Denied) not received
        {
        - If Uninhibit or Inhibit sent:
          then => ALARM

        }
      - elsewhile Uninhibit not sent nor Forced_Uninhibit received:
        - The Inhibit was accepted and we are within the Test Message cycle
        - **Scenario:** If a Local Inhibit message was inserted we should see the ACK from the Remote node. Then when the T20 expires, no Local Inhibit Test message will be sent. However, at the remote end, T21 expires and a Remote Inhibit Test message will be sent to the local node. Since the Local Node is not in the Inhibit mode, the Local node will respond with an Uninhibit message. This is the indicator that the original Link Inhibit message was inserted (or passed through the local node) to the Remote node.

      {

APPENDIX E
INTRUSION DETECTION ALGORITHMS

- when T20 expires: check for lack of Local Inhibit Test
  AND
- when T21 expires: check for Remote Inhibit Test received followed by Uninhibit sent
  - => soft alarm for 1st T20/T21 cycle
  - => threshold for multiple occurrence of 1st cycle Uninhibit

}
OR
{

- when T20 expires: check for Local Inhibit Test sent followed by no reaction received (still remote inhibited)
- when T21 expires: check for no action received (now remote UNinhibited)
- when T20 expires 2nd time check for Local Inhibit Test sent followed by Forced_Uninhibit received
- => ALARM (the Remote node should have sent a Forced_Uninhibit if it initiated the Uninhibit procedure. Since it only sent a Forced_Uninhibit as a response to the Local Inhibit test this may indicate the Remote node may be toggled back to an Uninhibited mode via alternate path)

}
}

- case: REMOTE_INHIBIT (Link_Inhibit received by node)

{

- while T14 not expired && Inhibit Ack not sent
  {
  - if Uninhibit received: ALARM

  }

- elsewhile Forced_Uninhibit not sent || Uninhibit not received: (the INHIBIT has been accepted)
  {
  - (Same conditions as LOCAL CASE only reverse sent and received designators)

  }

}

- **Link Inhibit Ack** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, SLC)
  - **Scenario:** no action is taken at the Local node when an unsolicited ACK is received (due to an inserted Link Inhibit => T1.111.4-38: no action
  - LINK_NEAREST_NEIGHBOR (check OPC and DPC are on collected link)
  - CORRELATE _TO_INHIBIT

- **Link Inhibit Denied** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, SLC)
  - LINK_NEAREST_NEIGHBOR (check OPC and DPC are on collected link)
  - CORRELATE _TO_INHIBIT_T14
  - Threshold Consecutive Attempts
    {
    - if >2 then ALARM

    }

- **Link Local Test Signal (T20 expires)** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, SLC)
  - CORRELATE _TO_INHIBIT_T20 (no Inhibit sent is ALARM)
  - if 1st Test && Forced Uninhibit received: soft ALARM

- **Link Remote Test Signal (T21 expires)**
  - CORRELATE _TO_INHIBIT_T21 (no Inhibit received is ALARM)
  - if 1st Test && Uninhibit received: soft ALARM

APPENDIX E
INTRUSION DETECTION ALGORITHMS

- **Transfer Controlled (congestion throttling)**
  - LINK_NEAREST_NEIGHBOR (check OPC and DPC are on collected link) && OPC_STP (only sent from STPs)

- **Signaling Route Set Congestion Test (T15/ T16 expires)**
  - CORRELATE_TO_TRANSFER_CONT

ISUP

- **Initial Address** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, CIC)
  - **Scenario**: store by CIC and TIMESTAMP use for correlation to REL. Illegal IAM messages in of themselves are not a significant threat to the network from a Service Disruption/Denial aspect unless a flooding attack was initiated to overwhelm network resources.

- **Address Complete** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, CIC)
- store by CIC and TIMESTAMP use for correlation

- **Release** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, CIC, CAUSE_CODE)
- Threshold # Occurrences
- check for VALID_DPC on link
- check for VALID_OPC on link
- check TRUNK_NEAREST_NEIGHBOR
- CORRELATE_TO_IAM
- check CAUSE_CODE
  - Code 1: unallocated number
  - Code 3: no route
  - Code 5: misdialled trunk prefix
  - Code 28: address incomplete
  - Code 31: normal unspecified
    {
    - CORRELATE_TO_ACM (ACM must occur prior to Normal Release)

    }
  - Code 79: service or option not implemented
  - Code 81: invalid Call Reference
  - Code 95: unspecified invalid message
  - Code 97: message type non-existent
  - Code 99, 100: invalid parameter
  - Code 111: unspecified protocol error

- CHECK_FOR_PATTERNS_CIC
  - **Scenario**: We are looking for the possibility that an attack on tearing down calls would have a pattern in the voice trunk numbers under attack. This would be found by looking for non-random patterns in the CIC parameter of consecutive REL messages. One possibility is to attack starting at low CIC numbers since calls are assigned from low to high
  - sequential numbering 0,1,2,3...N
  - switch specific numbering (accounting for switch specific card /shelf distributions)

- **Release Complete** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, CIC)
- CORRELATE_TO_REL || CORRELATE_TO_RESET || CORRELATE_TO_BLO
  - **Scenario**: RLC is possible response to receiving any above. So, if none of these messages preceded the RLC then it is an indicator that any of these messages was inserted at the RLC OPC node over a

APPENDIX E
INTRUSION DETECTION ALGORITHMS

different link. Furthermore, a Reset or Circuit Query response from the RLC indicates that the RLC was an unexpected message. This is further evidence that the RLC OPC node did not send the Release, Reset, or Blocking message.

{
- if FAIL
  {
- start timer and check for RESET || CIRCUIT QUERY (possible response to out of sequence RLC received at unaffected xchange due to inserted BLO)
- case: BLO sent in same direction: ALARM
  - **Scenario**: A Blocking message followed by an RLC observed in the same direction would occur only if the RLC OPC node received a Reset in a particular call state. Therefore the Reset message should have been observed before the BLO. If the Reset was not observed before this sequence than this indicates that the Reset was inserted at the RLC OPC node over a different link.

  }
}

- **Group Reset** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, CIC, RANGE)
- Check for pair of Group Resets within 5 seconds
- check for VALID_OPC/DPC
- check TRUNK_NEAREST_NEIGHBOR
- Threshold number of Occurrences within Timeperiod

- **Reset** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, CIC)
- check for VALID_OPC/DPC
- check TRUNK_NEAREST_NEIGHBOR
- Threshold number of Occurrences within Timeperiod
- CHECK_FOR_PATTERNS_CIC
  - sequential numbering 0,1,2,3...N
  - switch specific numbering (accounting for switch specific card /shelf distributions)
- set timer (15 seconds) and wait for Unequipped
- CORRELATE_TO_RLC
  - **Scenario**: A Reset or Circuit Query response from the RLC indicates that the RLC was an unexpected message. This is possible evidence that the RLC was the result of an inserted Release, Reset, or Blocking message at the RLC OPC node over a different link.

- **Group Blocking** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, CIC, RANGE)
- Check for pair of Group Blocking within 5 seconds
- check for VALID_OPC/DPC
- check TRUNK_NEAREST_NEIGHBOR
- Threshold number of Occurrences within Timeperiod

- **Blocking** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, CIC)
- check for VALID_OPC/DPC
- check TRUNK_NEAREST_NEIGHBOR
- Threshold number of Occurrences within Timeperiod
- set timer (5 min) and CORRELATE_TO_UNBLOCK (should not be held longer)
- CHECK_FOR_PATTERNS_CIC
- sequential numbering 0,1,2,3...N
  - switch specific numbering (accounting for switch specific card /shelf distributions)
- CORRELATE_TO_UBLA
  - **Scenario**: An Blocking message sent in response to an Unblocking Acknowledgment message indicates that the UBLA was unexpected since the CIC was not in a Local Unblocked state. This could

APPENDIX E
INTRUSION DETECTION ALGORITHMS

indicate that the UBLA was caused by an inserted Unblock to the UBLA OPC node over a different link
- Threshold number of occurrences

- **Blocking Ack** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, CIC)
- CORRELATE_TO_BLO (fail then: ALARM)
  - **Scenario**: If a BLA received without seeing a previous BLO then this indicates that a BLO may hae been inserted at the BLA OPC node

- **Unblock** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, CIC)
  - **Scenario**: The system monitors for this message primarily as indicator that some other message may not be legitimate. An illegal Unblocking message in of itself would only serve to bring CICs back INTO service prematurely; this is not perceived as a significant threat to the network.
- CLEAR_BLO_TIMER
  - **Scenario**: a circuit should only remain in a Blocked condition for no longer than approximately 5 minutes (usually due to maintenance actions)
- CORRELATE_TO_BLA
  - **Scenario**: An Unblocking message sent in response to a Blocking Acknowledgment message indicates that the BLA was unexpected since the CIC was not in a Local Blocked state. This could indicate that the BLA was caused by an inserted BLO to the BLA OPC node over a different link
  - Threshold number of occurrences
- Alarm aggregate to FAIL of BLA correlation to BLO

- **Unequipped Circuit** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, CIC)
  - **Scenario**: Unequipped response indicates that the Release, Reset or Blocking message was invalid since there is no circuit to reset. This is not very common since it indicates that the trunk status tables are out of sync or that the Release, Reset or Blocking messages are coming from a surce which has no knowledge of the trunking status. Therefore, a low threshold on the Unequipped messages is warranted.
- CORRELATE_TO_REL || CORRELATE_TO_RESET || CORRELATE_TO_BLO
- Threshold number of Occurrences within Timeperiod per CIC (low threshold)
- CHECK_FOR_PATTERNS_CIC
- sequential numbering 0,1,2,3...N
  - switch specific numbering (accounting for switch specific card /shelf distributions)

- **Circuit Query** (TIMESTAMP, LINK_ID, DIRECTION, OPC, DPC, CIC)
  - **Scenario**: Circuit Query sent as a response to a particular message (vice on a periodic polled basis) indicates a loss of sync in the trunking status tables. This is an event which should happen infrequently. It could also indicate that the node sending the offending message is not legitimate and is attempting to perform actions which are inconsistent with the actual trunk status. Alternatively, unsolicited Circuit Queries can indicate a "fishing expedition" by someone trying to build a database on the network trunking.
- check for VALID_OPC/DPC
- check TRUNK_NEAREST_NEIGHBOR
- Threshold number of Occurrences within Timeperiod
- CORRELATE_TO_RLC
  - Threshold number of occurrences by CIC
  - **Scenario**: A Reset or Circuit Query response from the RLC indicates that the RLC was an unexpected message. This is possible evidence that the RLC was the result of an inserted Release, Reset, or Blocking message at the RLC OPC node over a different link.

- **CORELLATE TO IAM** (assuming monitoring A-link at STP)
- {

APPENDIX E
INTRUSION DETECTION ALGORITHMS

- for both A-links
- {
    - lookup in Table IAM: enter CIC, look for previous collected corresponding IAM
        - where: (IAM_TIMESTAMP < REL_TIMESTAMP)
        - && ((OPC = IAM_DPC && DPC = IAM_OPC) || (OPC = IAM_OPC && DPC = IAM_DPC))
            - if found
            - { return PASS}
            - else
            - {return FAIL: ALARM}
- }
- }

- **TRUNK_NEAREST_NEIGHBOR** (This is based on individual C7RTE tables in the database)
- Overall: Check to see that the OPC and DPC of the ISUP messages:
    - have valid ISUP trunking relationships
    - were collected on the proper links

- Query database for C7RTE table for Point Code equal to either the message OPC or DPC
    - if Table Point Code = OPC (check for C7RTE Table for OPC)
    - {
    - search for record entry with DPC
        - if found
        - {
        - case A-link:
            - {
            - **Check_Current_Link**(RETURN_LinkID)
            - (verify A-link ID = Current Link ID)
            - }
        - case B-link:
            - {
            - **Lookup_B-Link**(RETURN_DPC)
            - (Query STP_C7RTE Table with DPC to obtain proper B-link ID for route to DPC)
              Check_Current_Link(RETURN_LinkID)
            - (verify B-link ID = Current Link ID)
            - }
        - else {RETURN_DPC_NOT_C7RTE} (the DPC was not a valid ISUP signaling partner)
    - }

    - elseif Table Point Code = DPC (check for C7RTE Table for DPC)
    - {
    - search for record entry with OPC
        - if found
        - {
        - case A-link:
            - {
            - **Check_Current_Link**(RETURN_LinkID)
            - (verify A-link ID = Current Link ID)
            - }
        - case B-link:
            - {
            - **Lookup_B-Link**(RETURN_OPC)
            - (Query STP_C7RTE Table with OPC to obtain proper B-link ID for route to OPC)
              Check_Current_Link(RETURN_LinkID)

APPENDIX E
INTRUSION DETECTION ALGORITHMS

- (verify B-link ID = Current Link ID)
- }
- else {RETURN_OPC_NOT_C7RTE} (the OPC was not a valid ISUP signaling partner)
- }

- else (Table Point Code did not match either OPC or DPC of message)
- { RETURN_INVALID_PC}

- SCCP UDT:
  - case: GTT = TRUE
    - {
    - lookup in GTE_SWITCH: enter DPC, look for corresponding CALLING PARTY PC
    - if found
    - { return pass}
    - else
    - {return fail}
    - }
    -
  - case:**UDT_GTT = TRUE** (SSN = 0)
  - {
    - lookup in Table IAM: enter CIC, look for previous collected corresponding IAM
    - where: (IAM_TIMESTAMP < REL_TIMESTAMP)
      - case: **REL_TOWARD_SSP** (IAM toward STP)
        - {
        - && (DPC = IAM_OPC || IAM_DPC = STP_PC)
          - if found
          - { return PASS}
          - else
          - {return FAIL ALARM }
        - }
      - case: **REL_TOWARD_STP** (IAM toward SSP)
        - {
        - && (OPC = IAM_DPC ||_??IAM_OPC = STP_PC??)
          - if found
          - { return PASS}
          - else
          - {return FAIL ALARM }
        - }

- Algorithms
  - Link Level
    - error message responses
      - FSN out of sequence
        - occurrence threshold
    - thresholding on each link by message type
      - number of occurrences
      - frequency of occurrences
      - patterns of circuits (REL , BLO)
        - sequential numbering 0,1,2,3...N
        - switch specific numbering (accounting for card /shelf distributions)
      - messages out of sequence (
      - patterns of links (Changeover, Transfer Prohibit/Restrict)

APPENDIX E
INTRUSION DETECTION ALGORITHMS

- Node Level
  - correlate messages across links/linksets
    - look for FISU/LSSU on links (Changeover, Transfer Prohibit/Restrict)
    - look for low level outages across links/linksets

Claims:

1. An apparatus for providing indications of attempted intrusion in a telecommunications signaling network, comprising:

means for receiving messages related to communications in the telecommunications signaling network;

means for applying intrusion rules to the messages in order to order to detect anomalies in the messages; and

means for reporting an indication of the detected anomalies.

2. The apparatus of claim I wherein the receiving means includes

means for receiving predefined test messages.

3. The apparatus of claim 1 wherein the receiving means includes

means for parsing and formatting the messages as required for the application of the intrusion rules.

4. The apparatus of claim I wherein the applying means includes

means for comparing the messages with information related to a known protocol for the telecommunications signaling network.

5. The apparatus of claim I wherein the reporting means includes

means for presenting in a user interface a topological representation of a portion of the telecommunications signaling network.

6. The apparatus of claim 5 wherein the reporting means includes means for presenting in the user interface indications of alarms representing the attempted intrusions.

7. An apparatus for determining a vulnerability of a telecommunications signaling network to attempted intrusions, comprising:

means for receiving rankings for particular parameters related to elements of the telecommunications signaling network;

means for applying vulnerability rules to the rankings in order to determine a

likelihood of an attempted intrusion into the corresponding elements of the telecommunications signaling network; and

means for reporting an indication of the likelihood of the attempted intrusions.

8. The apparatus of claim 7 wherein the receiving means includes means for presenting a user interface for receiving the rankings.

9. The apparatus of claim 7 wherein the applying means includes

means for combining the rankings according to particular criteria in order to produce numerical results providing indications of the likelihood of the attempted intrusions relative to the corresponding elements in the telecommunications signaling network.

10. The apparatus of claim 7 wherein the reporting means includes

means for reporting a most vulnerable node and a most vulnerable link in the telecommunications signaling network.

11. A method for providing indications of attempted intrusion in a telecommunications signaling network, comprising:

receiving messages related to communications in the telecommunications signaling network;

applying intrusion rules to the messages in order to order to detect anomalies in the messages; and

reporting an indication of the detected anomalies.

12. The method of claim 11 wherein the receiving includes

receiving predefined test messages.

13. The method of claim 11 wherein the receiving includes

parsing and formatting the messages as required for the application of the intrusion rules.

14. The method of claim 11 wherein the applying includes

comparing the messages with information related to a known protocol for the telecommunications signaling network.

15. The method of claim 11 wherein the reporting includes

presenting in a user interface a topological representation of a portion of the telecommunications signaling network.

16. The method of claim 15 wherein the reporting includes

presenting in the user interface indications of alarms representing the attempted intrusions.

17. A method for determining a vulnerability of a telecommunications signaling network to attempted intrusions comprising:

receiving rankings for particular parameters related to elements of the telecommunications signaling network, applying vulnerability rules to the rankings in order to determine a likelihood of an attempted intrusion into the corresponding elements of the telecommunications signaling network; and

reporting an indication of the likelihood of the attempted intrusions.

18. The method of claim 17 wherein the receiving includes

presenting a user interface for receiving the rankings.

19. The method of claim 17 wherein the applying includes

combining the rankings according to particular criteria in order to produce numerical results providing indications of the likelihood of the attempted intrusions relative to the corresponding elements in the telecommunications signaling network.

20. The method of claim 17 wherein the reporting includes

reporting a most vulnerable node and a most vulnerable link in the telecommunications signaling network.

AMENDED CLAIMS

[received by the International Bureau on 20.December 1999 (20.12.99); original claims 1,2,4,5,7,11 and 17 replaced by amended claims bearing the same number; new claims 21 to 26 added; remaining claims unchanged (5 pages)]

1. An apparatus for providing indications of attempted intrusion in a telecommunications signaling network, comprising:

means for receiving messages related to communications in the telecommunications signaling network;

means for applying intrusion rules to the messages in order to detect anomalies in the messages;

means for classifying the detected anomalies according to particular criteria; and

means for reporting an indication of the classifications of the detected anomalies.

2. The apparatus of claim 1 wherein the receiving means includes means for receiving predefined test messages.

3. The apparatus of claim 1 wherein the receiving means includes means for parsing and formatting the message as required for the application of the intrusion rules.

4. The apparatus of claim 1 wherein the applying means includes means for comparing the messages with information related to a known protocol for the telecommunications signaling network.

5. The apparatus of claim 1 wherein in the reporting means includes means for presenting in a user interface a topological representation of a portion of the telecommunications signaling network.

6. The apparatus of claim 5 wherein the reporting means includes means for presenting in the user interface indications of alarms representing the attempted intrusions.

7. An apparatus for determining a vulnerability of a telecommunications signaling network to attempted intrusions, comprising:

means for receiving rankings for particular parameters related to elements of the telecommunications signaling network;

means for applying vulnerability rules to the rankings in order to determine a likelihood of an attempted intrusion into the corresponding elements of the telecommunications signaling network, including means for determining a particular type of vulnerability of the corresponding elements; and

means for reporting an indication of the likelihood of the attempted intrusions, including means for determining, based upon the particular type of vulnerability, an action affecting the corresponding elements in order to reduce the likelihood of the attempted intrusion in the corresponding elements.

8. The apparatus of claim 7 wherein the receiving means includes means for presenting a user interface for receiving the rankings.

9. The apparatus of claim 7 wherein the applying means includes means for combining the rankings according to particular criteria in order to produce numerical results providing indications of the likelihood of the attempted intrusions relative to the corresponding elements in the telecommunications signaling network.

10. The apparatus of claim 7 wherein the reporting means includes means for reporting a most vulnerable node and a most vulnerable link in the telecommunications signaling network.

11. A method for providing indications of attempted intrusion in a telecommunications signaling network, comprising;

receiving messages related to communications in the telecommunications signaling network;

applying intrusion rules to the messages in order to detect anomalies in the messages;

classifying the detected anomalies according to particular criteria; and

reporting an indication of the classifications of the detected anomalies.

12. The method of claim 11 wherein the receiving includes receiving predefined test messages.

13. The method of claim 11 wherein the receiving includes parsing and formatting the messages as required for the application of the intrusion rules.

14. The method of claim 11 wherein the applying includes comparing the messages with information related to a known protocol for the telecommunications signaling network.

15. The method of claim 11 wherein the reporting includes presenting in a user interface a topological representation of a portion of the telecommunications signaling network.

16. The method of claim 15 wherein the reporting includes presenting in the user interface indications of alarms representing the attempted intrusions.

17. A method for determining a vulnerability of a telecommunications signaling network to attempted intrusions, comprising:

receiving rankings for particular parameters related to elements of the telecommunications signaling network;

applying vulnerability rules to the rankings in order to determine a likelihood of an attempted intrusion into the corresponding elements of the telecommunications signaling network, including determining a particular type of vulnerability of the corresponding elements; and

reporting an indication of the likelihood of the attempted intrusions, including determining, based upon the particular type of vulnerability, an action affecting the corresponding elements in order to reduce the likelihood of the attempted intrusion in the corresponding elements.

18. The method of claim 17 wherein the receiving includes presenting a user interface for receiving the rankings.

19. The method of claim 17 wherein the applying includes combining the rankings according to particular criteria in order to produce numerical results providing indications of the likelihood of the attempted intrusions relative to the corresponding elements in the telecommunications signaling network.

20. The method of claim 17 wherein the reporting includes reporting a most vulnerable node and a most vulnerable link in the telecommunications signaling network.

21. The apparatus of claim 1 wherein the reporting means includes means for generating, based upon the intrusion rules, a time-stamped listing of the classifications of anomalies and the corresponding messages.

22. The apparatus of claim 1 wherein the reporting means includes means for generating statistics, based on particular criteria, concerning the messages.

23. An apparatus for providing indications of attempted intrusion in a telecommunications signaling network, comprising:

means for receiving a first message related to communications in the telecommunications signaling network and referring to a particular link in the network;

means for applying an intrusion rule to the first message in order to detect anomalies in the first message, including determining if a second message of a predefined type was previously detected on the particular link; and

means for reporting an indication of the detected anomalies.

24. The method of claim 11 wherein the reporting includes generating, based upon the intrusion rules, a time-stamped listing of the classifications of anomalies and the corresponding messages.

25. The method of claim 11 wherein the reporting includes generating statistics, based on particular criteria, concerning the messages.

26. A method for providing indications of attempted intrusion in a telecommunications signaling network, comprising:

receiving a first message related to communications in the telecommunications signaling network and referring to a particular link in the network;

applying an intrusion rule to the first message in order to detect anomalies in the first message, including determining if a second message of a predefined type was previously detected on the particular link; and

reporting an indication of the detected anomalies.

FIG. 1

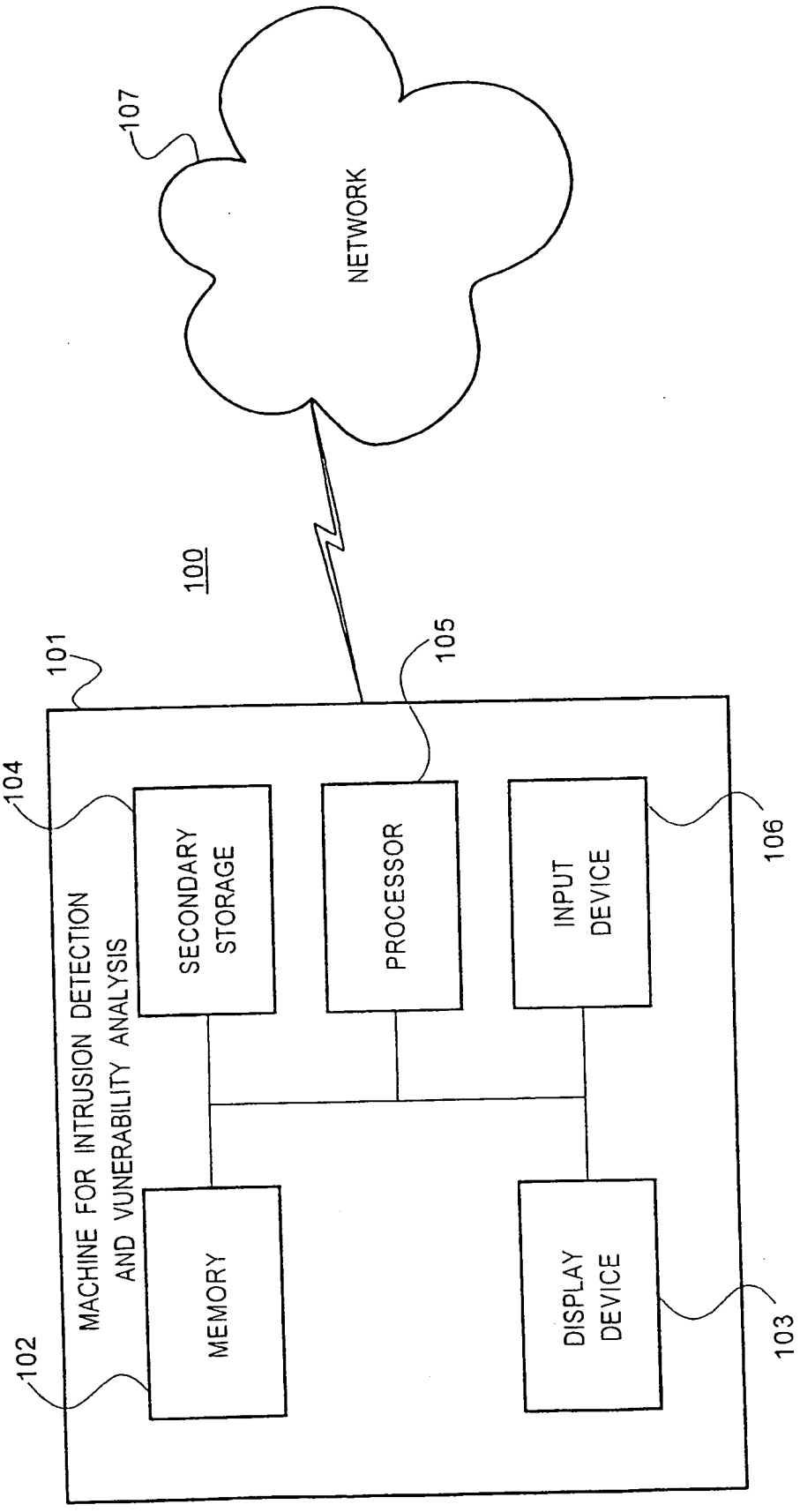

NETWORK
107
100
101
105
104
SECONDARY STORAGE
PROCESSOR
INPUT DEVICE
106
MACHINE FOR INTRUSION DETECTION AND VUNERABILITY ANALYSIS
MEMORY
DISPLAY DEVICE
102
103

FIG. 2

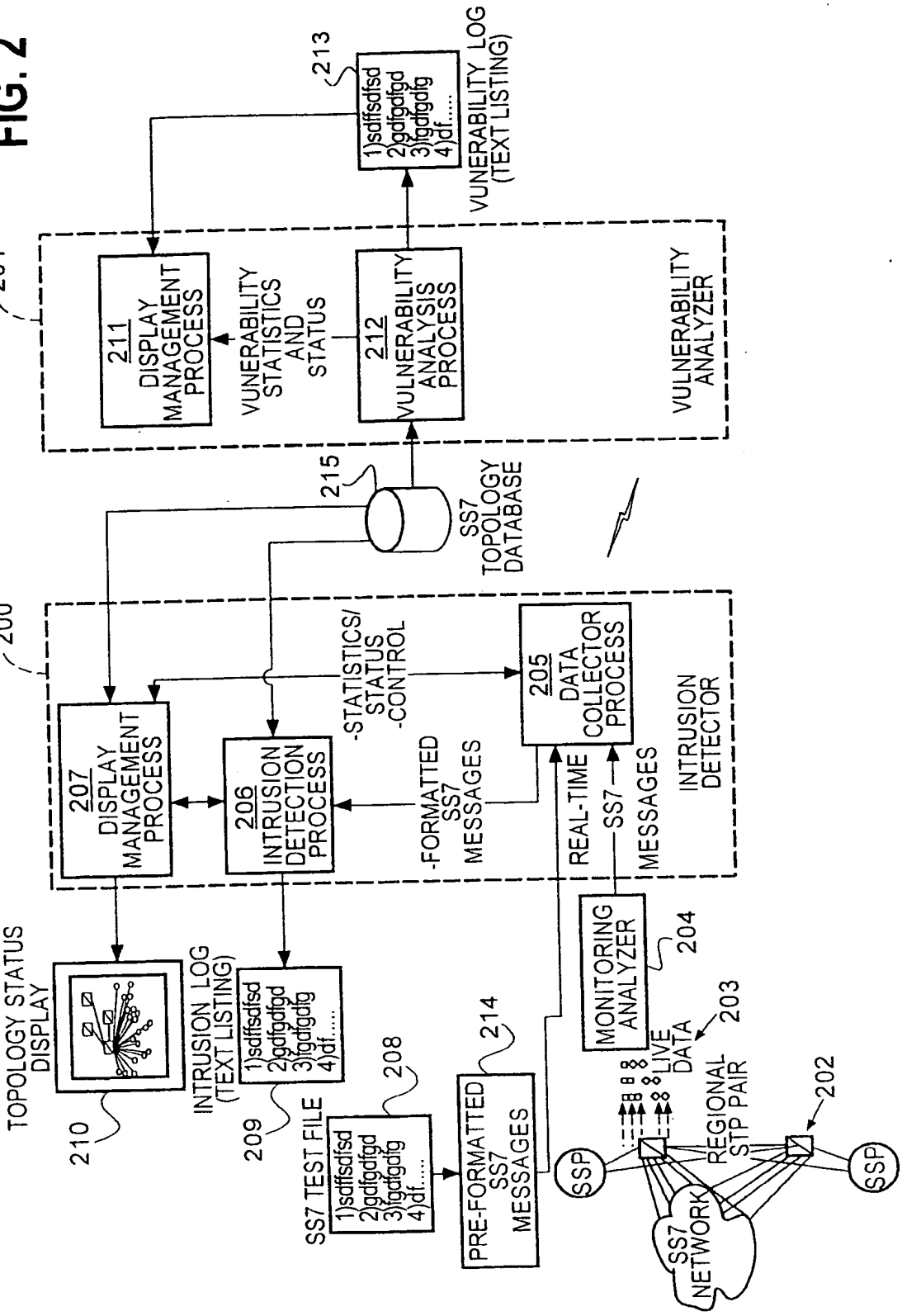

201
VULNERABILITY ANALYZER
211 DISPLAY MANAGEMENT PROCESS
VUNERABILITY STATISTICS AND STATUS
212 VULNERABILITY ANALYSIS PROCESS
213
1)sdffsdfsd 2)gdfgdfgd 3)fgdfgdfg 4)df.....
VUNERABILITY LOG (TEXT LISTING)
215
SS7 TOPOLOGY DATABASE
200
INTRUSION DETECTOR
207 DISPLAY MANAGEMENT PROCESS
206 INTRUSION DETECTION PROCESS
205 DATA COLLECTOR PROCESS
-STATISTICS/ STATUS -CONTROL
-FORMATTED SS7 MESSAGES
REAL-TIME SS7 MESSAGES
MONITORING ANALYZER
204
LIVE DATA
203
202
REGIONAL STP PAIR
SSP
SSP
SS7 NETWORK
TOPOLOGY STATUS DISPLAY
210
INTRUSION LOG (TEXT LISTING)
209
SS7 TEST FILE
208
PRE-FORMATTED SS7 MESSAGES
214

FIG. 3

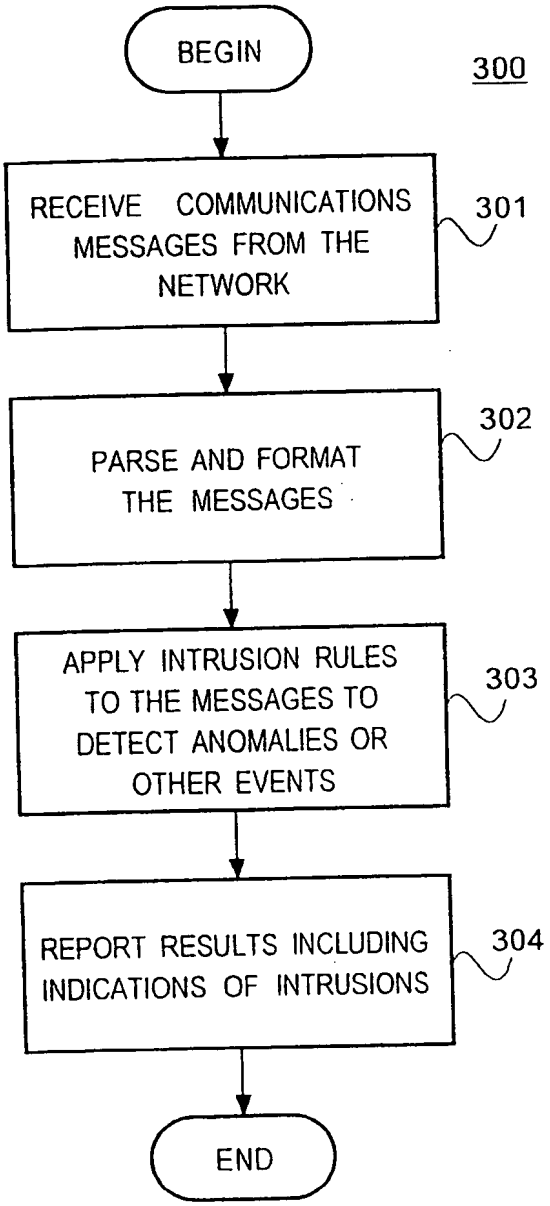
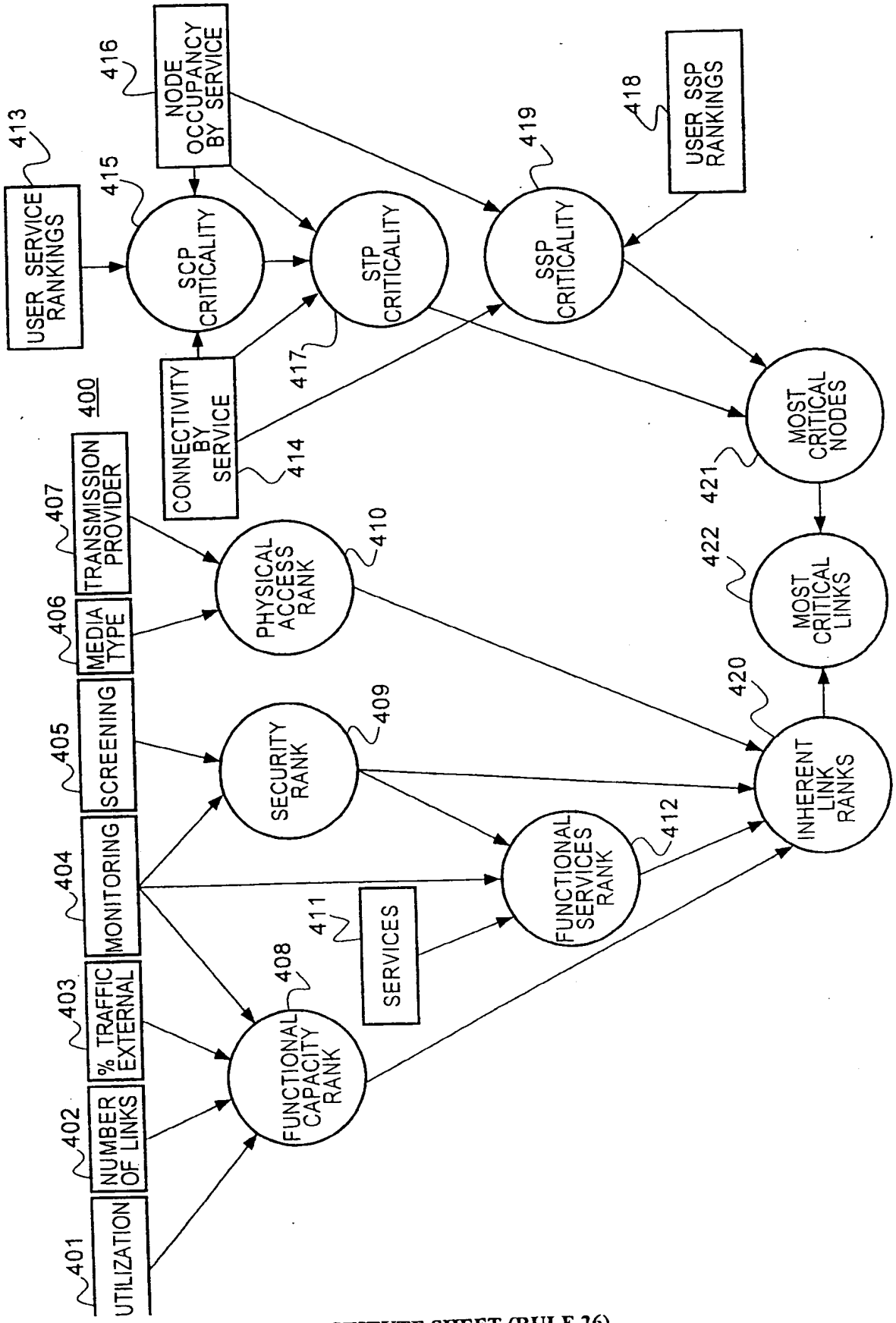

BEGIN
300
RECEIVE COMMUNICATIONS MESSAGES FROM THE NETWORK
301
PARSE AND FORMAT THE MESSAGES
302
APPLY INTRUSION RULES TO THE MESSAGES TO DETECT ANOMALIES OR OTHER EVENTS
303
REPORT RESULTS INCLUDING INDICATIONS OF INTRUSIONS
304
END

FIG. 4


400
401
UTILIZATION
402
NUMBER OF LINKS
403
% TRAFFIC EXTERNAL
404
MONITORING
405
SCREENING
406
MEDIA TYPE
407
TRANSMISSION PROVIDER
408
FUNCTIONAL CAPACITY RANK
409
SECURITY RANK
410
PHYSICAL ACCESS RANK
411
SERVICES
412
FUNCTIONAL SERVICES RANK
413
USER SERVICE RANKINGS
414
CONNECTIVITY BY SERVICE
415
SCP CRITICALITY
416
NODE OCCUPANCY BY SERVICE
417
STP CRITICALITY
418
USER SSP RANKINGS
419
SSP CRITICALITY
420
INHERENT LINK RANKS
421
MOST CRITICAL NODES
422
MOST CRITICAL LINKS

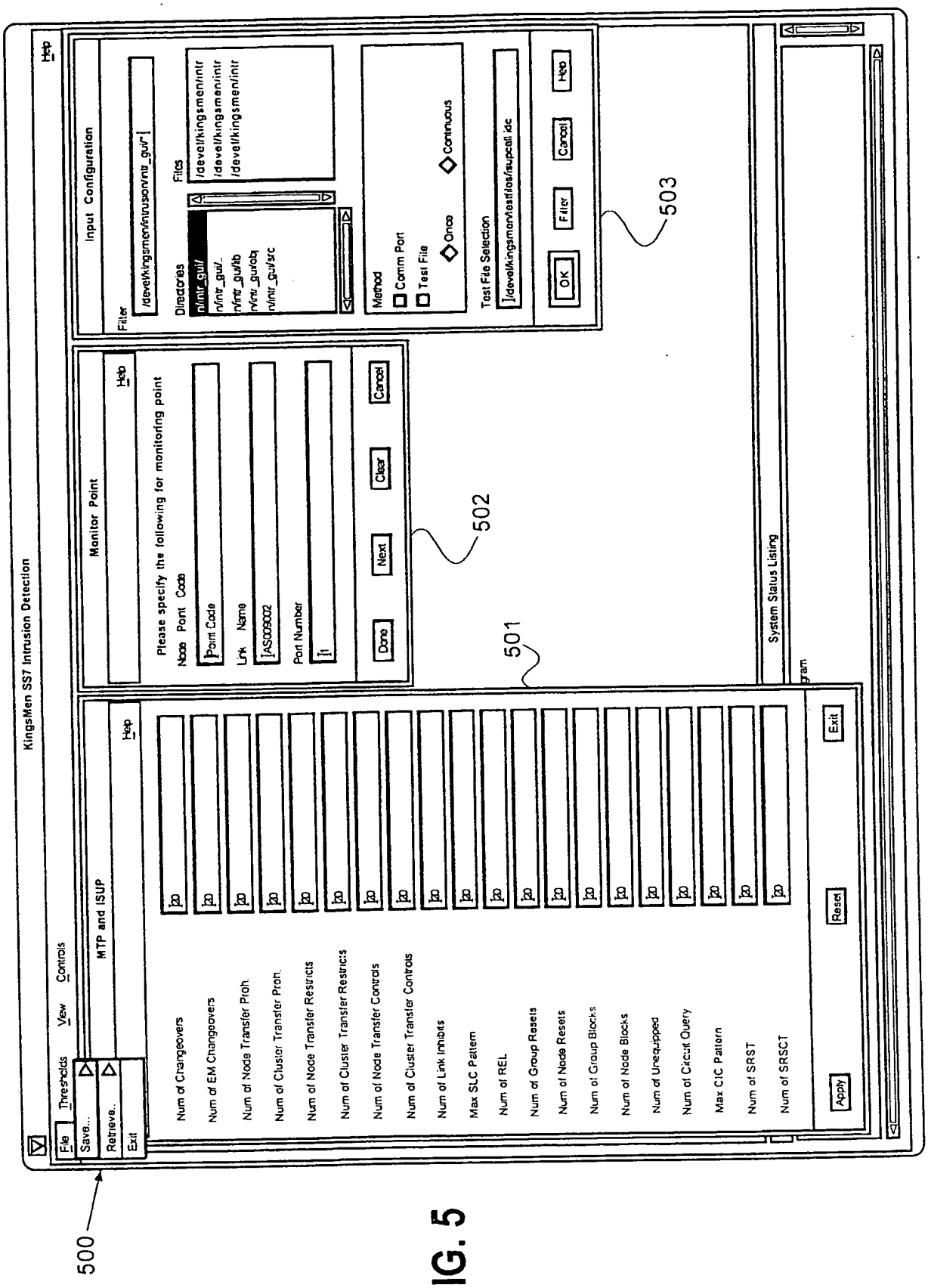

KingsMen SS7 Intrusion Detection
File
Thresholds
View
Controls
Help
Save...
Retrieve...
Exit
MTP and ISUP
Num of Changeovers
Num of EM Changeovers
Num of Node Transfer Proh
Num of Cluster Transfer Proh
Num of Node Transfer Restricts
Num of Cluster Transfer Restricts
Num of Node Transfer Controls
Num of Cluster Transfer Controls
Num of Link Inhibits
Max SLC Pattern
Num of REL
Num of Group Resets
Num of Node Resets
Num of Group Blocks
Num of Node Blocks
Num of Unequipped
Num of Circuit Query
Max CIC Pattern
Num of SRST
Num of SRSCT
Apply
Reset
Exit
Monitor Point
Please specify the following for monitoring point
Node Point Code
Point Code
Link Name
AS0080002
Port Number
1
Done
Next
Clear
Cancel
Input Configuration
Filter
/devel/kingsmen/intrusion/intr_gui/
Directories
Files
/devel/kingsmen/intr
Method
Comm Port
Test File
Once
Continuous
Test File Selection
/devel/kingsmen/testfiles/isupcall.idc
OK
Filter
Cancel
System Status Listing
500
501
502
503

FIG. 5

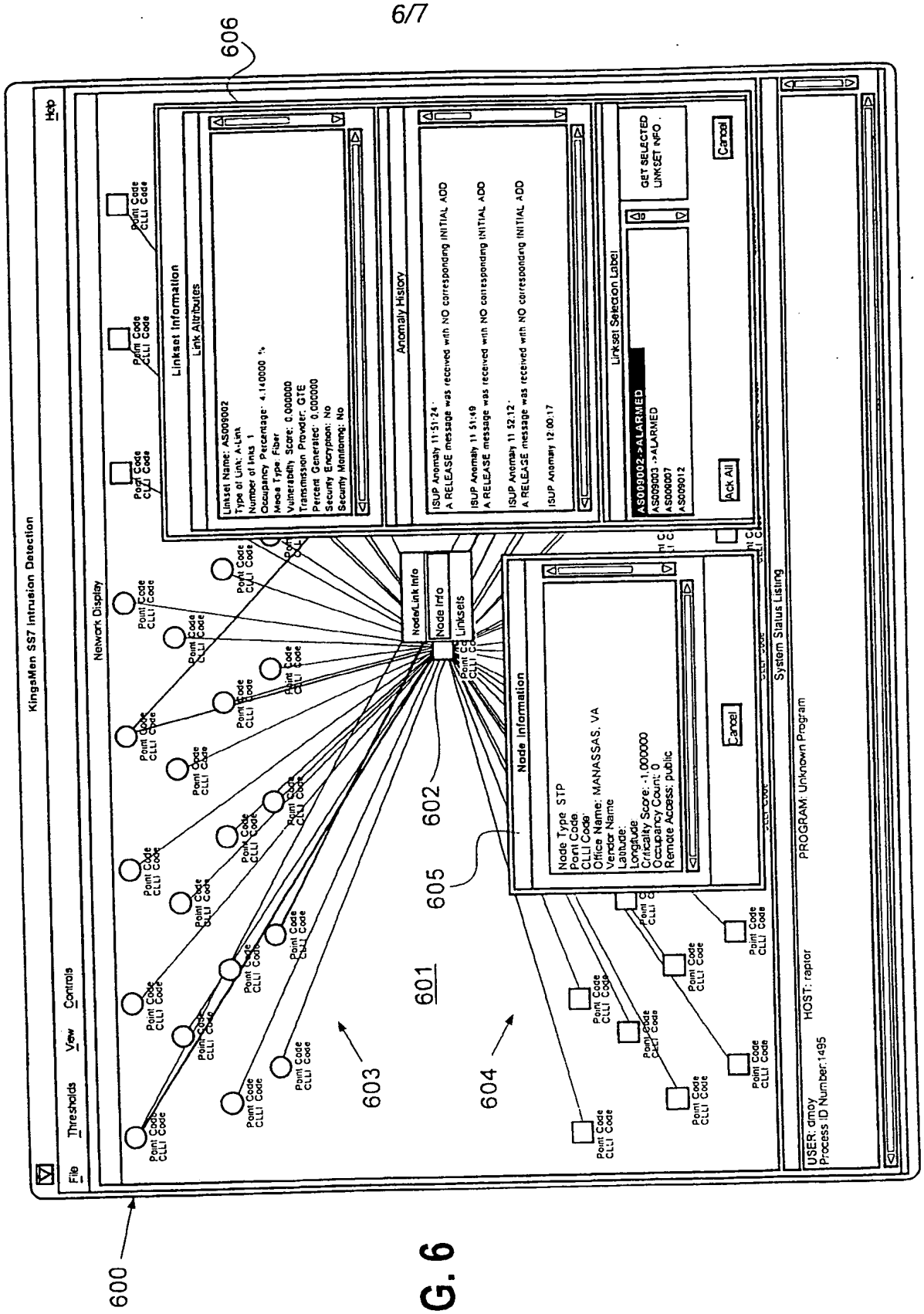

606
KingsMen SS7 Intrusion Detection
File Thresholds View Controls Help
Network Display
Linkset Information
Link Attributes
Linkset Name: AS009002
Type of Link: A-Link
Number of links: 1
Occupancy Percentage: 4.140000 %
Media Type: Fiber
Vulnerability Score: 0.000000
Transmission Provider: GTE
Percent Generated: 0.000000
Security Encryption: No
Security Monitoring: No
Anomaly History
ISUP Anomaly 11:51:24:
A RELEASE message was received with NO corresponding INITIAL ADD
ISUP Anomaly 11:51:49
A RELEASE message was received with NO corresponding INITIAL ADD
ISUP Anomaly 11:52:12:
A RELEASE message was received with NO corresponding INITIAL ADD
ISUP Anomaly 12:00:17
Linkset Selection Label
AS009002->ALARMED
AS009003 ->ALARMED
AS009007
AS009012
GET SELECTED LINKSET INFO
Cancel
Ack All
Node/Link Info
Node Info
Linksets
Node Information
Node Type: STP
Point Code:
CLLI Code:
Office Name: MANASSAS, VA
Vendor Name:
Latitude:
Longitude:
Criticality Score: -1.000000
Occupancy Count: 0
Remote Access: public
Cancel
System Status Listing
HOST: raptor
PROGRAM: Unknown Program
USER: dmoy
Process ID Number:1495
Point Code
CLLI Code
600
601
602
603
604
605

FIG. 6

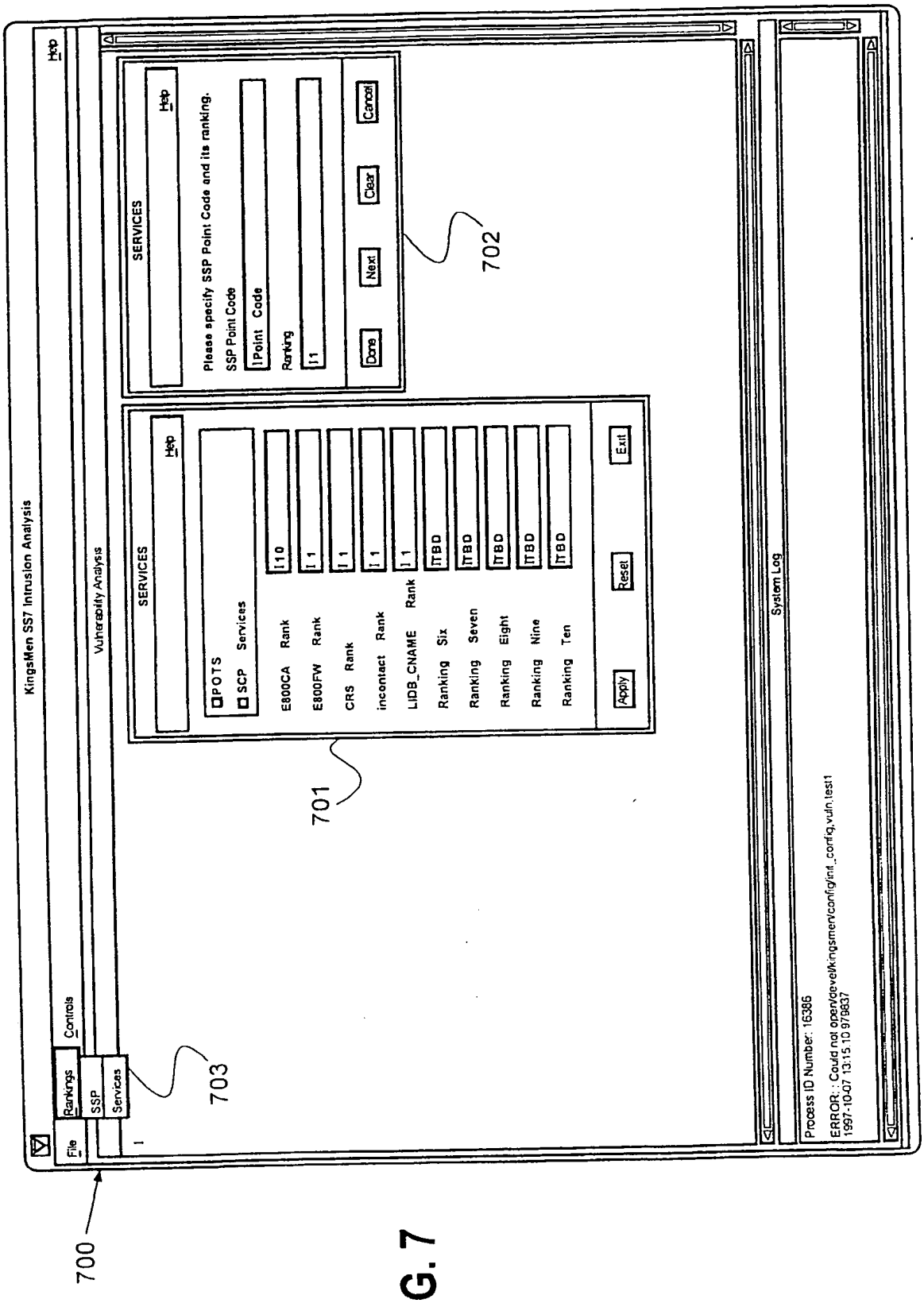

KingsMen SS7 Intrusion Analysis
Help
Controls
Vulnerability Analysis
File
Rankings
SSP
Services
1
SERVICES
Help
Please specify SSP Point Code and its ranking.
SSP Point Code
Point Code
Ranking
11
Done
Next
Clear
Cancel
SERVICES
Help
POTS
SCP Services
E800CA Rank
E800FW Rank
CRS Rank
incontact Rank
LIDB_CNAME Rank
Ranking Six
Ranking Seven
Ranking Eight
Ranking Nine
Ranking Ten
110
1 1
1 1
1 1
1 1
ITBD
ITBD
ITBD
ITBD
ITBD
Apply
Reset
Exit
System Log
Process ID Number: 16386
ERROR:: Could not open/dev/kingsmen/config/int_config.vuln.test1
1997-10-07 13:15:10 978837
700
701
702
703

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/17408

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04J 3/14; F06F 11/00

US CL :Please See Extra Sheet.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 370/230, 235, 236, 252, 385, 463; 709/223, 224, 225; 713/200, 201

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS
search item: security, firewall, intrusion

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5,621,889 A (LERMUZEAUX et al) 15 April 1997, col. 3, line 13-col. 8, line 25.	1-6, 11-16
Y	US 5,623,601 A (VU) 22 April 1997, col. 7, line 10-col. 14, line 9.	1-20
Y	US 5,757,924 A (FRIEDMAN et al) 26 May 1998, col. 7, line 7-col. 10, line 24.	1-20
Y	US 5,440,723 A (ARNOLD et al) 08 August 1995, col. 4, line 60-col. 10, line 10.	1-20
Y	US 5,586,254 A (KONDO et al) 17 December 1996, col. 6, line 6-col. 12, line 40.	1-20

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 22 SEPTEMBER 1999	Date of mailing of the international search report 19 OCT 1999
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer SOON-DONG HYUN Telephone No. (703) 305-3900

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

In...national application No.
PCT/US99/17408

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

370/230, 235, 236, 252, 385, 463; 709/223, 224, 225; 713/200, 201